RUCKUS FastIron Software Upgrade Guide, 10.0.00

Supporting FastIron Software Release 10.0.00

Part Number: 53-1005755-02
Publication Date: 15 December 2022

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **5**
- Contacting RUCKUS Customer Services and Support 5
  - What Support Do I Need? 5
  - Open a Case 5
  - Self-Service Resources 6
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
  - Notes, Cautions, and Safety Warnings 7
- Command Syntax Conventions 7

About This Document **9**
- New in This Document 9
- Supported Hardware 9

Software Upgrade **11**
- Software Upgrade Procedure Overview 11
- General Considerations for Upgrade to FastIron Release 10.0.00 or Later 12
  - Configuration Migration Considerations 12
  - Management VLAN and Management Port Considerations 14
  - Spanning Tree Protocol Configuration 18
  - Considerations for Multicast 19
  - Default Forwarding Profile Migration for ICX 7550 21
- General Considerations for Upgrade to FastIron Release 09.0.10a or Later 22
  - Preparing for the Upgrade 22
  - Transition to cli timeout Command 23
- Initial Steps 23
  - Determining the Current Flash and Boot Image Versions 24
  - Determining the Current Licenses Installed 24
- Upgrade Considerations for Licensed Features 25
  - Upgrade Considerations for the Layer 3 Premium License 25
  - Upgrade Considerations for MACsec Licenses 26
- Upgrade Considerations for ACLs 27
  - MAC ACLs 27
  - ACL Logging Upgrade Considerations 28
  - ACL Accounting Upgrade Considerations 28
  - ACL- Related Changes When Upgrading to FastIron 08.0.95 or Later 28
- Upgrade Considerations for Stacks 32
  - Changes to Upgrade for Stacking from FastIron 08.0.90 32
  - Downgrading a Stack to a Release Prior to FastIron 09.0.10a 33
  - Recovering a Broken Stack After a Downgrade from FastIron 09.0.10a or Later 34
- Upgrade Process 35
  - Mandatory Upgrade Steps from a Pre-08.0.80 Non-UFI Version to a 09.0.10a or Later UFI Version 36
  - Upgrading from a UFI Version to a Later UFI Version 44
- Using a USB Device for Image Download 44
  - Upgrade Using the Manifest File in the USB Drive 45

Auto-Download Using a USB Device 45
Copying the UFI and Manifest Packages from System Flash to a USB Drive 46
OS Prompt Recovery Procedures 46
Software Recovery 47
Recovering Software 47
In-Service Software Upgrade 51
In-Service Software Upgrade Overview 51
ISSU Limitations and Considerations 51
Recommended Stack Topology for ISSU 51
How ISSU Works When Upgrading Stack Units 52
Pre-ISSU Compatibility Checks for a Traditional Stack 54
Upgrading a Stack with ISSU 54
ISSU Errors 59
Error Recovery 60
Manual Error Recovery 60

Preface

- Contacting RUCKUS Customer Services and Support 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
- Command Syntax Conventions 7

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Document

- New in This Document 9
- Supported Hardware 9

New in This Document

NOTE

Features introduced in FastIron release 09.0.10d are not supported in FastIron release 10.0.00 but will be supported in FastIron release 10.0.10.[1]

TABLE 2 Summary of Enhancements in FastIron Release 10.0.00

Feature	Description	Reference
RUCKUS ICX 8200	**New**: Added support for RUCKUS ICX 8200 devices.	Throughout the guide
Discontinuation of support for a separate switch image	**Updated**: This release and future releases support a single image for ICX platforms that provides both switching and routing functionality. As a result, support for a separate switch ("Layer 2") image is discontinued.	General Considerations for Upgrade to FastIron Release 10.0.00 or Later on page 12 References have been removed throughout the guide
Unsupported hardware	**Updated**: This release and future releases do not support RUCKUS ICX 7150, 7250, and 7450 devices.	References have been removed throughout the guide
Updates to address defects	**Updated**: Minor updates on content throughout to address defects.	All chapters
Minor editorial updates	**Updated**: Minor editorial updates were made throughout the guide.	All chapters

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 8200 Switches
- RUCKUS ICX 7850 Switches
- RUCKUS ICX 7650 Switches
- RUCKUS ICX 7550 Switches

For information about what models and modules these devices support, refer to the hardware installation guide for the specific product family.

[1] Support for Network Segmentation, Dynamic Bootstrap Protocol (BOOTP) Support, DHCP - IP to Physical Port Mapping, VXLAN with Routing in and out of tunnels (RIOT), VXLAN - VXLAN Network Identifier (VNI) Scale Enhancement, VXLAN Remote Site Monitoring and Redundancy, Proactive Monitoring of Cable Signal Errors and Loggin

Software Upgrade

- Software Upgrade Procedure Overview 11
- General Considerations for Upgrade to FastIron Release 10.0.00 or Later 12
- General Considerations for Upgrade to FastIron Release 09.0.10a or Later 22
- Initial Steps 23
- Upgrade Considerations for Licensed Features 25
- Upgrade Considerations for ACLs 27
- Upgrade Considerations for Stacks 32
- Upgrade Process 35
- Using a USB Device for Image Download 44
- OS Prompt Recovery Procedures 46
- Software Recovery 47

Software Upgrade Procedure Overview

You can upgrade FastIron software in several ways: through a manual step-by-step process, through a manifest file, or through a Unified FastIron Image (UFI).

TABLE 3 Upgrade Behavior by Platform

Upgrading From Release	Image Type	Upgrade to FI 10.0.00	Behavior
08.0.90 and later (ICX 7650 and 7850) 08.0.95 and later (ICX 7550)	Router	No special procedure required	No change
08.0.70 (ICX 7650)	Router	Upgrade to FastIron 08.0.80a UFI image and then to FastIron 10.0.00	No change
08.0.80 and later (ICX 7650) 08.0.95 and later (ICX 7550)	Switch	No special procedure required	Configuration gets updated to equivalent commands in router image. Refer to Mandatory Upgrade Steps from a Pre-08.0.80 Non-UFI Version to a 09.0.10a or Later UFI Version on page 36 for more details
08.0.70 (ICX 7650)	Switch	Upgrade to FastIron 08.0.80a UFI image and then to FastIron 10.0.00	Configuration gets updated to equivalent commands in router image. Refer to Mandatory Upgrade Steps from a Pre-08.0.80 Non-UFI Version to a 09.0.10a or Later UFI Version on page 36 for more details

Before updating, review these considerations:

- Beginning with FastIron release 10.0.0, a switch ("Layer 2") image will no longer be provided for ICX devices. Only the router ("Layer 3") image will be available. On upgrade to FastIron 10.0.00, the configuration of any ICX devices operating with the switch image will automatically be translated to the equivalent router image configuration.

- The UFI image copy is the recommended software upgrade method for both standalone devices and traditional stacks. All hardware plaforms support UFI images for software upgrade. Only the ICX 7650 supports both non-UFI images and UFI images.

1. Preliminary checks. For any upgrade, review the information in General Considerations for Upgrade to FastIron Release 10.0.00 or Later on page 12 and General Considerations for Upgrade to FastIron Release 09.0.10a or Later on page 22, and then follow the instructions in Initial Steps on page 23 to determine the current software versions, license requirements, and instructions on where to download the software.

   Unless configured, syslogs do not persist across reloads.
2. Upgrade the software. For a step-by-step upgrade, refer to Upgrade Process on page 35.

   NOTE
   For a stack, you can perform a full manual upgrade for each unit, or you can download the software as described in Upgrade Process on page 35, followed by an in-service software upgrade for the stack as described in In-Service Software Upgrade on page 51. Be sure to check ISSU Limitations and Considerations on page 51 before performing an in-service software upgrade.

General Considerations for Upgrade to FastIron Release 10.0.00 or Later

Beginning with FastIron release 10.0.0, a switch ("Layer 2") image will no longer be provided for ICX devices. Only the router ("Layer 3") image will be available. On upgrade to FastIron 10.0.00, the configuration of any ICX devices operating with the switch image will automatically be translated to the equivalent router image configuration.

The switch image for the ICX 7550 and ICX 7650 is discontinued in FastIron 10.0.00. When upgrading these devices there isan automated migration which will change the configuration after the upgrade.

Configuration related to the following features will be modified:

- Management VLAN and Management Port
- Spanning Tree Protocol (STP)
- Multicast
- Forwarding Profile for the ICX 7550
- IP address is configured at the interface level
- Support for management VLAN and the default gateway is discontinued

Before upgrade, also review the information in General Considerations for Upgrade to FastIron Release 09.0.10a or Later on page 22.

Configuration Migration Considerations

Configuration related to certain features is modified during migration to the FastIron 10.0.0 or later router image. The following table provides details.

TABLE 4 FastIron Release 10.0.00 Configuration Migration Considerations

Feature	FastIron 9.0.10x and Before Behavior	FastIron 10.0.00 and Later Behavior	Notes
DHCP-client (v4)	Switch Image: • DHCP client enabled at global level • No interface level configuration Command to enable dhcp client – **Ip dhcp-client enable** Command to disable dhcp client – **no ip dhcp-client enable** Router Image: • DHCP client enabled at global level on a VE • Enabled at interface level including the lease setting Command to enable dhcp client – **no ip dhcp-client disable** Command to disable dhcp client – **ip dhcp-client disable**	Router Image: • DHCP client enabled at global level on a VE • Enabled at interface level including the lease setting Command to enable dhcp client – **no ip dhcp-client disable** Command to disable dhcp client – **ip dhcp-client disable**	DHCP-client is enabled by default at global level, but DHCP-client can be enabled at interface level in router image as well. The **no ip dhcp-client enable** command will be migrated to **ip dhcp-client disable** command during the upgrade.

TABLE 4 FastIron Release 10.0.00 Configuration Migration Considerations (continued)

Feature	FastIron 9.0.10x and Before Behavior	FastIron 10.0.00 and Later Behavior	Notes

FDP	Switch Image:
	• FDP is enabled at the global level
	Example:
	`9000Switch(config) #fdp`
	`  advertise  Control advertising of address type`
	`  holdtime  Specify the holdtime (in sec) to be sent in packets`
	`  run  Enable FDP globally`
	`  timer  Specify the rate at which FDP packets are sent (in sec)`
	Router Image:
	• FDP is enabled at the interface level
	Example:
	`9000Router(config)# fdp`
	`  holdtime  Specify the holdtime (in sec) to be sent in packets`
	`  run  Enable FDP globally`
	`  timer  Specify the rate at which FDP packets are sent (in sec)`
		Router Image:
		• FDP is enabled at the interface level
		Example:
		`  holdtime`
		`Specify the holdtime (in sec) to be sent in packets`
		`  run`
		`Enable FDP globally`
		`  timer`
		`Specify the rate at which FDP packets are sent (in sec`
			In the switch image, FDP advertise (both IPv4 and IPv6) is configured at global level, but in the router image, it is configured at interface level.
			After the upgrade from a switch image to FastIron 10.0.0, you must manually configure the FDP advertise command on individual interfaces.

Management VLAN and Management Port Considerations

For releases prior to FastIron 10.0.00, the IP address can be configured at the global level with the switch image. With the router image, the IP address must be configured at the interface level.

FastIron software will determine whether the management port is being used for accessing the device. Based on the detection, IP address configuration will be translated to equivalent router image commands according to the table below:

TABLE 5 Management Configuration Scenarios for DHCP (IPv4)

Management VLAN Status	Prior to FastIron 10.0.00	Upgrade to FastIron 10.0.00 or Later

Configured	• Management-VLAN configured
	• DHCP Client configured
	Example:
	`vlan 45`
	` untagged ethernet 1/1/4`
	` management-vlan`
	` default-gateway 45.1.1.1 1 dynamic`
	`!`
	`ip address 45.1.1.2 255.255.255.0 dynamic`
	`!`
		Configuration added:
		• VE is created on the VLAN
		• VE is configured as a DCHP client
		- ip dhcp client ve
		Example:
		`ip dhcp-client ve 45`
		`!`
		`int ve 45`
		` ip address 45.1.1.2 255.255.255.0 dynamic`
		`!`
		`ip route 0.0.0.0/0 45.1.1.1 distance 254 dynamic`

Not Configured	• DHCP Client configured
	• No management-vlan configured
	• DHCP Server reachable on data port in any VLAN
	Example:
	`vlan 45`
	` untagged ethernet 1/1/4`
	` default-gateway 45.1.1.1 1 dynamic`
	`!`
	`ip address 45.1.1.2 255.255.255.0 dynamic`
	`!`
		VE is created on the default VLAN and will be configured as DHCP client
		Example:
		`!`
		`interface ve 1`
		` ip address 45.1.1.2 255.255.255.0 dynamic`
		`!`
		`ip route 0.0.0.0/0 45.1.1.1 distance 254 dynamic`

	• DHCP Client configured
	• No management-vlan configured
	• DHCP Server reachable on management port
	• Basically no configuration for management access.
	Example:
	`ip default-gateway 45.1.1.1 1 dynamic`
	`!`
	`ip address 45.1.1.2 255.255.255.0 dynamic`
	`!`
		DHCP server reachable over management port
		Example:
		`int management 1`
		` ip address 45.1.1.2 255.255.255.0 dynamic`
		`!`
		`ip route 0.0.0.0/0 45.1.1.1 distance 254 dynamic`

TABLE 6 Management Configuration Scenarios for Static IP Address

Management VLAN Status	Prior to FastIron 10.0.00	Router Image for FastIron 10.0.00 or Later

Confiigured	• Switch has static IP address configured along with management VLAN
	• Default gateway is reachable via management port
	Example:
	`!`
	`vlan 9`
	` untagged ethernet 1/1/9`
	` management-vlan`
	` default-gateway 10.177.133.129 1`
	` default-gateway 9.1.1.2 1`
	` default-gateway 19.1.1.2 2`
	`!`
	`ip address 10.177.133.138`
	`255.255.255.128`
	`!`
		• IP address will be configured on the management port
		• Default gateway will be converted to a static route
		Example:
		`!`
		`int management 1`
		` ip address 10.177.133.138`
		`255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.129`

	Default gateway reachable via data port
	Example:
	`!`
	`vlan 9`
	` untagged ethernet 1/1/9`
	` management-vlan`
	` default-gateway 9.1.1.2 1`
	` default-gateway 20.1.1.2 2`
	`!`
	`ip address 9.1.1.1 255.255.255.0`
	`!`
		Example:
		• VE is created on the VLAN
		• IP address will be configured on the VE
		• Default gateway configuration will be converted to a static route
		`!`
		`int ve 9`
		` ip address 9.1.1.1 255.255.255.0`
		`!`
		`ip route 0.0.0.0/0 9.1.1.2`

	Both the data port and management port is used to access the device
	Example:
	`!`
	`ip address 10.177.133.138`
	`255.255.255.128`
	`ip default-gateway 10.177.133.129`
	`!`
		FastIron selects the port through which the default gateway is reachable
		Example:
		`!!`
		`int management 1`
		`ip address 10.177.133.138`
		`255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.129`
		`(or)`
		`!`
		`int ve 1`
		`ip address 10.177.133.138`
		`255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.129`

	No gateway configured
	`!`
	`ip address 9.1.1.1 255.255.255.0`
	`!`
		IP address is assigned to the management port
		`!`
		`int management 1`
		` ip address 9.1.1.1 255.255.255.0`
		`!`

TABLE 6 Management Configuration Scenarios for Static IP Address (continued)

Management VLAN Status	Prior to FastIron 10.0.00	Router Image for FastIron 10.0.00 or Later

Not Configured	Default gateway is reachable via management port
	Example:
	`ip address 10.177.133.138 255.255.255.128`
	`ip default-gateway 10.177.133.129`
		• IP address is assigned to the management port
		• Gateway will be converted to default route
		Example:
		`!`
		`int management 1`
		`ip address 10.177.133.138 255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.12`

	• Default gateway is reachable via a data port
	• Port is not part of VLAN
	Example:
	`!`
	`interface ethernet 1/1/9`
	`!`
	`ip address 9.1.1.1 255.255.255.0`
	`ip default-gateway 9.1.1.2`
		• VE interface is created on the default VLAN
		• IP address is assigned to this VE interface
		• Gateway will be converted to default route
		Example:
		`!`
		`int ve 1`
		`ip address 9.1.1.1 255.255.255.0`
		`!`
		`ip route 0.0.0.0/0 9.1.1.2`

	• Default gateway reachable via a data port
	• Port is part of VLAN
	Example:
	`!`
	`vlan 100`
	`untagged ethernet 1/1/9`
	`!`
	`ip address 10.1.1.1 255.255.255.0`
	`ip default-gateway 10.1.1.2`
		• VE interface is created on the corresponding VLAN
		• IP address is assigned to the VE interface
		Example:
		`!`
		`vlan 100`
		`untagged ethernet 1/1/9`
		`!`
		`int ve 100`
		`ip address 10.1.1.1 255.255.255.0`
		`!`
		`ip route 0.0.0.0/0 10.1.1.2`

	Both the data port and management port is used to access the device
	Example:
	`!`
	`ip address 10.177.133.138 255.255.255.128`
	`ip default-gateway 10.177.133.129`
	`!`
		FastIron selects the port through which the default gateway is reachable.
		Example:
		`!`
		`int management 1`
		`ip address 10.177.133.138 255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.129`
		`(or)`
		`!`
		`int ve 1`
		`ip address 10.177.133.138 255.255.255.128`
		`!`
		`ip route 0.0.0.0/0 10.177.133.129`

TABLE 6 Management Configuration Scenarios for Static IP Address (continued)

Management VLAN Status	Prior to FastIron 10.0.00	Router Image for FastIron 10.0.00 or Later

Not Configured Continued	• No Gateway configured
	• Device is getting accessed through any port (same subnet as Switch IP
	Example:
	`!`
	`ip address 9.1.1.1 255.255.255.0`
	`!`
		Management IP address is assigned to the management port
		Example:
		`!`
		`int management 1`
		`ip address 9.1.1.1 255.255.255.0`
		`!`

	• Default VLAN is configured
	• Gateway is reachable through a data port
	Example:
	`!`
	`default-vlan-id 100`
	`!`
	`ip address 9.1.1.2 255.255.255.0`
	`ip default-gateway 9.1.1.1`
		IP address is assigned to the VE of the default VLAN
		Example:
		`!`
		`int ve 100`
		`ip address 9.1.1.2 255.255.255.0`
		`!`
		`ip route 0.0.0.0/0 9.1.1.1`

Spanning Tree Protocol Configuration

The switch image by default runs spanning-tree and attaches a new spanning instance as and when a new VLAN is created. Since this is a system default behavior, spanning-tree is not generated under a VLAN in the running configuration file.

However for the router image, VLAN does not run spanning-tree by default. Unless spanning-tree string is explicitly present under the VLAN configuration, the router image will not run spanning-tree under that VLAN. During upgrade, the running configuration shall be modified to generate the spanning-tree under the VLAN configuration (once the system detects that the original running-config was from a switch image) as shown below:

TABLE 7

Switch Image Sample Configuration	Configuration After Mingration to FastIron 10.0.00 or Later

`vlan 10`
`tagged ethernet 1/1/1`
 	
`vlan 20`
`tagged ethernet 1/1/1`
 	
`vlan 30`
`no spanning-tree`
`tagged ethernet 1/1/1`
 	
`vlan 40`
`spanning-tree 802.1w`
`tagged ethernet 1/1/1`
	`vlan 10`
	`spanning-tree`
	`tagged ethernet 1/1/1`
	
	`vlan 20`
	`spanning-tree`
	`tagged ethernet 1/1/1`
	
	`vlan 30`
	`no spanning-tree`
	`tagged ethernet 1/1/1`
	
	`vlan 40`
	`spanning-tree 802.1w`
	`tagged ethernet 1/1/1`

Running config has MSTP configuration	No change in the running configuration
Running config has single spanning-tree configured	No change in the running configuration

Considerations for Multicast

For MLD snooping no changes or additional rules are needed. Rules for selecting the IP address to send MLD query packets in order of decreasing priority include:

1. Snooping VLAN querier address
2. Switch IPv6 Link Local Address+

For IGMP snooping, if querier-address is not configured specifically then IGMP snooping uses the IP address configured on these interfaces as source address in the query packets (querier address) as per the rules in below table.

TABLE 8 Rules for Selecting the IP Address to Send IGMP Query Packets

Switch Image (Before FastIron 10.0.00)	Router Image (Before FastIron 10.0.00)	10.0.00 Single Router Image
1. Snooping VLAN querier address 2. Device IP address	1. Snooping VLAN Querier address 2. Snooping VLAN VE IP address 3. First loopback interface IP address	1. Snooping VLAN querier address 2. Snooping VLAN VE IP address 3. First loopback interface IP address 4. First VE IP address Added to support upgrade from switch image to the single router image. 5. OB management port IP address Added to support upgrade from switch image to the single router image.

Example: IP address configured on VE interface after upgrade

Before Upgrade on Switch Image

```
vlan 9
 untagged ethernet 1/1/9
 management-vlan
 default-gateway 9.1.1.1 1
 default-gateway 20.1.1.2 2
!
ip address 9.1.1.2 255.255.255.0
!
vlan 1000 by port
 tagged ethe 3/1/11 lag 102
 multicast active
 multicast6 active
!
!
device# show ip multicast vlan 1000
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255,
                      Leave Wait=2, Robustness=2

VL1000: dft V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
  My Query address: 9.1.1.2 (management)
  e3/1/11   has    0 grp, QR, default V2
  lg102     has    0 grp, QR, default V2 trunk
device#
```

After Upgrade to 10.0.00 Router Image

```
vlan 9 by port
 untagged ethernet 1/1/9
 spanning-tree
!
int ve 9
 ip address 9.1.1.2 255.255.255.0
!
ip route 0.0.0.0/0 9.1.1.1
!
vlan 1000 by port
 tagged ethe 3/1/11 lag 102
 multicast active
 multicast6 active
!
device# show ip multicast vlan 1000
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255,
                      Leave Wait=2, Robustness=2

VL1000: dft V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port
  My Query address: 9.1.1.2 (ve/loopback/management)
  Edge ports: ALL
  Non-Edge ports: NONE
  e3/1/11   has    0 grp, QR, default V2
  lg102     has    0 grp, QR, default V2 trunk
device#
```

Example: IP address configured on Out of Band Management interface after upgrade

Before Upgrade on Switch Image

```
ip address 9.1.1.2 255.255.255.0
ip default-gateway 9.1.1.1
!
vlan 1000 by port
 tagged ethe 3/1/11 lag 102
 multicast active
 multicast6 active
!
device# show ip multicast vlan 1000
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255,
                      Leave Wait=2, Robustness=2

VL1000: dft V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port,
  My Query address: 9.1.1.2 (management)
  e3/1/11   has    0 grp, QR, default V2
  lg102     has    0 grp, QR, default V2 trunk
device#
```

After Upgrade to 10.0.00 Router image

```
int management 1
 ip address 9.1.1.2 255.255.255.0
!
ip route 0.0.0.0/0 9.1.1.1
!
vlan 1000 by port
 tagged ethe 3/1/11 lag 102
 multicast active
 multicast6 active
!
ICX# show ip multicast vlan 1000
Version=2, Intervals: Query=125, Group Age=260, Max Resp=10, Other Qr=255,
                      Leave Wait=2, Robustness=2

VL1000: dft V2, vlan cfg active, 0 grp, 0 (*G) cache, no rtr port
  My Query address: 9.1.1.2 (ve/loopback/management)
  Edge ports: ALL
  Non-Edge ports: NONE
  e3/1/11   has    0 grp, QR, default V2
  lg102     has    0 grp, QR, default V2 trunk
device#
```

Default Forwarding Profile Migration for ICX 7550

The forward table scale numbers (system max) are different between the default router forwarding profile and the switch default profile. During upgrade from switch image to the router image, profile2 will be chosen this migrates to the router image forwarding profile that is closest to the switch image default forwarding table numbers.

TABLE 9

Prior to FastIron 10.0.00 Switch Image Forwarding Profile	FastIron 10.0.00 Route Image Migrated to Forwarding Profile: Profile2
ICX7550-48 Switch# show default values forwarding profile: profile2 mac :98304 ip-route :0 ip6- route :0 igmp-snoop-mcache :8192 igmp-snoop- group-addr :8192 mld-snoop-mcache :2048 mld-snoop- group-addr :8192 pim-hw-mcache :0 pim6-hw- mcache :0 hw-ip-next-hop :21504	ICX7550-48 Router# show forwarding-profile details Parameter-name profile1 profile2 profile3 mac 16384 114688 32768 ip-route 97280 8192 21504 ip6-route 8192 2048 17408 igmp-snoop-mcache 6144 6144 6144 igmp-snoop-group-addr 6144 6144 6144 mld-snoop-mcache 2048 2048 2048 mld-snoop-group-addr 8192 8192 8192 pim-hw-mcache 6144 6144 6144 pim6-hw-mcache 2048 2048 2048 hw-ip-next-hop 21504 21504 21504 Default YES NO NO

General Considerations for Upgrade to FastIron Release 09.0.10a or Later

Because of the many software design and CLI changes implemented in FastIron 09.0.10a, downgrading to a previous release is complex and may produce unexpected results.

NOTE
Downgrading software is not recommended.

IMPORTANT REMINDER
Be sure you have backed up your previous startup configuration before you begin any upgrade or downgrade process.

Preparing for the Upgrade

Before upgrading to FastIron 09.0.10a or a later release, RUCKUS strongly recommends the following steps:

- Make a backup copy of the ICX startup configuration (the startup-config file). This copy will be used if a downgrade to a previous release is necessary. If you have made changes to the running configuration, you may also want to save a copy of the running-config file.

  The following example saves a copy of a FastIron 08.0.95 startup configuration and a running configuration and stores them on the TFTP server, identified by its IP address.

```
ICX# copy startup-config tftp 10.176.198.42 old-8095-cfg
ICX# Upload startup-config to TFTP server done.
ICX# copy running-config tftp 10.176.198.42 old-8095-run-cfg
ICX# Upload running-config to TFTP server done.
```

NOTE
A FastIron 09.0.10a or later startup-config file does not parse properly for a pre-09.0.10 release due to design changes. When you downgrade, configuration changes, including the user account configuration and stack configuration, among others, will be lost.

- Consult the FastIron release notes and user documentation for the current release about significant software design changes that may need to be taken into consideration.

NOTE
If you are upgrading an ICX switch for the first time from a version earlier than FastIron 08.0.95, RUCKUS recommends that you upgrade to FastIron 08.0.95d as the intermediate version and then upgrade to FastIron 09.0.10a or later. This step is required to ensure that the FPGA version is compatible with the target release.

NOTE
If you are upgrading to FastIron 09.0.10a or later and the ICX device contains the **service password-encryption sha1** configuration, any users who are configured with SHA1 encryption are removed during the upgrade.

NOTE
If you are upgrading to FastIron 09.0.10a or later, it is recommended to re-configure the DHCP server address pool, and to configure the lease count with the number of leases specific to the address pool. Refer to "Configuring the Number of Leases for the Address Pool" in the *RUCKUS FastIron DHCP Configuration Guide* for more information.

Transition to cli timeout Command

The **cli timeout** command is introduced in FastIron 09.0.10a and replaces the **ip ssh idle-time**, **telnet timeout**, and **console timeout** commands. The following rules apply when converting a timer configuration from earlier releases upon upgrade to FastIron 09.0.10a or later:

- The default value for the **cli timeout** command is 2 minutes, which applies if none of the replaced commands has s prior configuration. After 2 minutes, by default, a console, Telnet, or SSH session times out.
- Previously, the default for console timeout was 0, which meant the console session never timed out. Starting with FastIron 09.0.10a, if you do not want sessions to time out, you must set the **cli timeout** value to 0.
- Upon upgrade to FastIron 09.0.10a or a later release, the **cli timeout** value is acquired from previous configurations in the following order of priority:
  - **ip ssh idle-time** configuration
  - **telnet timeout** configuration
  - **console timeout** configuration

Initial Steps

NOTE
You must upgrade to the boot code that supports the current release. Refer to **Image File Names** in the release notes for detailed information.

NOTE
Beginning with FastIron release 10.0.00, manifest file copy is no longer supported for the switch image (Layer 2). The router image (Layer 3) must be used for the manifest file copy process to work correctly.

If you are upgrading from FastIron release 08.0.90 or later, RUCKUS recommends using SCP to transfer files.

Determining the Current Flash and Boot Image Versions

To determine the current boot and flash image versions installed on a device, enter the **show version** command at any level of the CLI.

```
ICX7550-48P Router# show flash
Stack unit 1:
  Compressed Pri Code size = 65736224, Version:09.0.10dT243 (GZR09010d_b12.bin)
  Compressed Sec Code size = 72551212, Version:10.0.00T243 (GZR10000_b389.bin)
  Compressed Pri Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
  Compressed Sec Boot Code size = 1081856, Version:10.2.01T245 (gzu1021b63)
  Code Flash Free Space = 2137440256
Stack unit 2:
  Compressed Pri Code size = 65736224, Version:09.0.10dT243 (GZR09010d_b12.bin)
  Compressed Sec Code size = 72551212, Version:10.0.00T243 (GZR10000_b389.bin)
  Compressed Pri Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
  Compressed Sec Boot Code size = 1081856, Version:10.2.01T245 (gzu1021b63)
  Code Flash Free Space = 2176720896
Stack unit 3:
  Compressed Pri Code size = 65736224, Version:09.0.10dT243 (GZR09010d_b12.bin)
  Compressed Sec Code size = 72551212, Version:10.0.00T243 (GZR10000_b389.bin)
  Compressed Pri Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
  Compressed Sec Boot Code size = 1081856, Version:10.2.01T245 (gzu1021b63)
  Code Flash Free Space = 2064109568
ICX7550-48P Router#
```

Determining the Current Licenses Installed

Use the **show version** or the **show license** command to display the licenses installed on the device.

```
ICX7550-48P Router# show version
  Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 5: compiled on Jul  4 2022 at 22:57:26 labeled as GZR09010d
      (65658632 bytes) from Primary GZR09010d.bin (UFI)
        SW: Version 09.0.10dT243
      Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
       Compiled on Thu Apr 21 11:22:29 2022
    UNIT 4: compiled on Jul  4 2022 at 22:57:26 labeled as GZR09010d
      (65658632 bytes) from Primary GZR09010d.bin (UFI)
        SW: Version 09.0.10dT243
      Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
    UNIT 6: compiled on Jul  4 2022 at 22:57:26 labeled as GZR09010d
      (65658632 bytes) from Primary GZR09010d.bin (UFI)
        SW: Version 09.0.10dT243
      Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)

  HW: Stackable ICX7550-48-POE
==============================================================================
UNIT 4: SL 1: ICX7550-48 48-port Management Module
      Serial  #:FML4208R00Y
      Software Package: ICX7550_L3_SOFT_PACKAGE
      Current License: l3-prem
==============================================================================
UNIT 4: SL 2: ICX7550-QSFP 2-port 80G Module
==============================================================================
UNIT 4: SL 3: ICX7600-2X40GQ 2-port 80G Module
      Serial  #:EZG3320N0B3
==============================================================================
UNIT 5: SL 1: ICX7550-48P POE 48-port Management Module
      Serial  #:FMN4210R010
      Software Package: ICX7550_L3_SOFT_PACKAGE
      Current License: l3-prem
      P-ASIC  8: type B371, rev 03  Chip BCM56371_A2
==============================================================================
UNIT 5: SL 2: ICX7550-QSFP 2-port 80G Module
==============================================================================
UNIT 5: SL 3: ICX7600-2X40GQ 2-port 80G Module
      Serial  #:EZG4207R004
==============================================================================
```

```
UNIT 6: SL 1: ICX7550-48P POE 48-port Management Module
      Serial  #:FMN4210R016
      Software Package: ICX7550_BASE_L3_SOFT_PACKAGE
      Current License: l3-base
==========================================================================
UNIT 6: SL 2: ICX7550-QSFP 2-port 80G Module
==========================================================================
UNIT 6: SL 3: ICX7600-2X40GQ 2-port 80G Module
      Serial  #:EZG4207R006
==========================================================================
 1700 MHz ARMv8 Cortex-A72 processor 857 MHz bus
   16 MB boot flash memory
    4 GB code flash memory
    4 GB DRAM
STACKID 5  system uptime is 18 hour(s) 51 minute(s) 9 second(s)
STACKID 4  system uptime is 18 hour(s) 51 minute(s) 12 second(s)
STACKID 6  system uptime is 18 hour(s) 51 minute(s) 8 second(s)
The system started at 03:50:31 GMT+00 Wed Jul 06 2022

The system : started=warm start   reloaded=by "reload"
My stack unit ID = 5, bootup role = active

ICX7550-48P Router# show license
Unit  License Name    L3 Premium Port Speed Upgrade   Speed    Ports    MACsec
4     l3-prem         Yes        NA                   NA       NA       No
5     l3-prem         Yes        NA                   NA       NA       No
6     l3-base         No         NA                   NA       NA       No
```

Obtaining Software Licenses

NOTE
For complete instructions on how to generate a license, refer to the *RUCKUS FastIron Software Licensing Guide*.

1. If required, generate a new license from the License Management page on the RUCKUS Support website. If you are upgrading to a different type of image that uses a different license from the one already installed on the device, generate a separate license file.
2. Download the required software images for the target release from the Software Downloads page on the RUCKUS Support website. For the list of software image files available for a specific release, refer to the release notes for that specific release.

Upgrade Considerations for Licensed Features

Upgrading or downgrading to a different FastIron release can affect the availability of licensed features on the system. Review the following upgrade considerations before upgrading.

Upgrade Considerations for the Layer 3 Premium License

Beginning with FastIron 08.0.80, all Layer 3 Premium licenses are Self-Authenticated Upgrade (SAU) licenses.

Upgrading a System Without a Layer 3 Premium License from FastIron 08.0.70 or Earlier Releases

Layer 3 Premium licensed features are not available until the user has enabled the Layer 3 Premium SAU license. Without the Layer 3 Premium license, the Layer 3 licensed features cannot be used.

In an upgrade from FastIron 08.0.70 or earlier releases to FastIron 08.0.80 or later releases, the system enables the Layer 3 Base license package automatically, which means all Layer 3 premium features are disabled.

However, if the system does not have a Layer 3 Premium XML license and Layer 3 Premium features are configured, these L3 features will be lost after the upgrade. In order to avoid losing Layer 3 configurations, perform one of the following actions before or after the upgrade:

- Before upgrading the system, check the license compliance status. Purchase and install the Layer 3 Premium XML license on the device if needed. Always back up the configuration, and keep a backup of all license files.
- Before upgrading the system, back up the configuration. After the upgrade, enable the Layer 3 Premium SAU license and copy the configuration back to the system.
- After upgrading the system, immediately enable the Layer 3 Premium SAU license, but do not save the configuration, and then reload. After the system is back up, the Layer 3 Premium configuration should be back as it was before the upgrade.

  NOTE
  In this case, the running configuration is lost, but the Layer 3 premium configuration remains in the startup configuration as long as the user does not enter the **write mem** command after the upgrade.

In a stacking configuration, if Layer 3 licensed features are required then a valid Layer 3 Premium license must be installed on all members of the stack.

If the active unit has an XML Layer 3 Premium license installed, the Layer 3 Premium configuration should remain the same after the upgrade, but member units without a Layer 3 Premium XML license will enter a non-operational state. To prevent member units from becoming non-operational, copy the Layer 3 Premium XML license to relevant units before the upgrade, or enable the Layer 3 Premium SAU license on relevant units after the upgrade.

If the active unit does not have a Layer 3 Premium XML license, the configuration of any premium Layer 3 features will be lost after the upgrade. Use one of the three preceding methods to prevent the loss of or to recover the Layer 3 configuration.

ICX Device with an Existing Layer 3 Premium XML License

If there is an existing Layer 3 Premium XML license on the device, the system will automatically enable the Layer 3 Premium SAU license upon upgrade to 08.0.80, and Layer 3 feature configuration will be retained. All Layer 3 features will function as before the upgrade.

All XML license files will be preserved in case the device is loaded with a non-SAU license image (that is, in case of a downgrade).

Upgrade Considerations for MACsec Licenses

Beginning with FastIron 08.0.80, all Layer 3 Premium licenses are Self-Authenticated Upgrade (SAU) licenses.

Upgrading a System Without a Layer 3 Premium License from FastIron 08.0.70 or Earlier Releases

Layer 3 Premium licensed features are not available until the user has enabled the Layer 3 Premium SAU license. Without the Layer 3 Premium license, the Layer 3 licensed features cannot be used.

In an upgrade from FastIron 08.0.70 or earlier releases to FastIron 08.0.80 or later releases, the system enables the Layer 3 Base license package automatically, which means all Layer 3 premium features are disabled.

However, if the system does not have a Layer 3 Premium XML license and Layer 3 Premium features are configured, these L3 features will be lost after the upgrade. In order to avoid losing Layer 3 configurations, perform one of the following actions before or after the upgrade:

- Before upgrading the system, check the license compliance status. Purchase and install the Layer 3 Premium XML license on the device if needed. Always back up the configuration, and keep a backup of all license files.
- Before upgrading the system, back up the configuration. After the upgrade, enable the Layer 3 Premium SAU license and copy the configuration back to the system.

- After upgrading the system, immediately enable the Layer 3 Premium SAU license, but do not save the configuration, and then reload. After the system is back up, the Layer 3 Premium configuration should be back as it was before the upgrade.

  NOTE
  In this case, the running configuration is lost, but the Layer 3 premium configuration remains in the startup configuration as long as the user does not enter the **write mem** command after the upgrade.

In a stacking configuration, if Layer 3 licensed features are required then a valid Layer 3 Premium license must be installed on all members of the stack.

If the active unit has an XML Layer 3 Premium license installed, the Layer 3 Premium configuration should remain the same after the upgrade, but member units without a Layer 3 Premium XML license will enter a non-operational state. To prevent member units from becoming non-operational, copy the Layer 3 Premium XML license to relevant units before the upgrade, or enable the Layer 3 Premium SAU license on relevant units after the upgrade.

If the active unit does not have a Layer 3 Premium XML license, the configuration of any premium Layer 3 features will be lost after the upgrade. Use one of the three preceding methods to prevent the loss of or to recover the Layer 3 configuration.

ICX Device with an Existing Layer 3 Premium XML License

If there is an existing Layer 3 Premium XML license on the device, the system will automatically enable the Layer 3 Premium SAU license upon upgrade to 08.0.80, and Layer 3 feature configuration will be retained. All Layer 3 features will function as before the upgrade.

All XML license files will be preserved in case the device is loaded with a non-SAU license image (that is, in case of a downgrade).

Upgrade Considerations for ACLs

This section describes the software upgrade changes related to access control lists (ACLs). For more detailed information, refer to the *RUCKUS FastIron Security Configuration Guide*.

MAC ACLs

When upgrading from a previous major release to FastIron 08.0.95 or a later release, all the existing MAC filters and their bindings in the startup configuration are migrated to MAC ACLs.

MAC filters defined by the **mac filter** command in releases prior to FastIron 08.0.95 that are bound to a particular physical interface or LAG with the **mac filter-group** command are converted into MAC ACLs, which are configured from FastIron 08.0.95 using the **mac access-list** command. The **mac access-list** command allows permt and deny filter statements to be created in MAC ACL configuration mode. The filters in a MAC ACL will appear in the same order as defined in the MAC filters.

NOTE
Permit and deny statements for MAC ACLs have a syntax similar to IP ACLs. For more information, refer to the *RUCKUS FastIron Command Reference Guide*.

An existing MAC filter that is not in any binding group is translated and added into a default MAC ACL. The **mac filter-group** command, used for binding MAC filters on an interface and LAG in releases prior to FastIron 08.0.95, has been replaced with the **mac access-group** command. The **mac access-group** command binds MAC ACLs to a physical interface, LAG, VLAN, and so on. The MAC filter functionality remains intact after an upgrade. Beginning with FastIron 08.0.95, the **mac filter** and **mac filter-group** commands are deprecated.

ACL Logging Upgrade Considerations

In FastIron 08.0.95 and later, the **acl-logging** command for IPv4 and **logging-enable** command for IPv6 are replaced by the **logging enable** command. ACL logging is configurable only at the binding level and is used in conjunction with the **log** keyword at the filter level for IPv4, IPv6, and MAC ACLs.

After an upgrade to FastIron 08.0.95 or a later, the following changes occur if ACL logging is enabled:

- IPv4 ACL: If logging is enabled for an interface before upgrade, then logging will be enabled for all the existing ACLs on the interface to which they are bound and their ingress and egress directions after the upgrade.
- IPv6 ACL: If logging is enabled for an IPv6 ACL and the interface to which it is bound before upgrade, then logging will be enabled for all bindings of the existing ACLs in both the ingress and egress directions after the upgrade.
- MAC ACL: If MAC filter logging is enabled on the global level before upgrade, then log option will be added to all MAC ACL rules after the upgrade. Also, if logging is enabled for a filter group binding to an interface before upgrade, then logging will be enabled for the respective bindings corresponding to the filter group and interface combination in the ingress direction after the upgrade.

  NOTE
  ACL logging is not supported for ACLs applied to outbound traffic.

ACL Accounting Upgrade Considerations

ACL accounting will be enabled by default for all filters. In FastIron 08.0.95 and later, the **enable-accounting** command has been modified to **enable accounting**.

After an upgrade to FastIron 08.0.95 or a later, the following changes occur for ACL accounting:

- IPv4 ACL: If accounting is enabled for an IPv4 ACL before upgrade, then it is enabled for all the filters that belong to that ACL after the upgrade.
- IPv6 ACL: If accounting is enabled for an IPv6 ACL before upgrade, then it is enabled for all the filters that belong to that ACL after the upgrade.
- MAC ACL: If accounting is enabled for a MAC filter before upgrade, then it is enabled for any MAC ACL that contains the filter after the upgrade.

The ACL accounting configuration of the MAC filter will migrate seamlessly during the upgrade. The accounting configuration for MAC filters that are not bound to any interface will be lost during upgrade and must be configured again for any resulting MAC ACL.

ACL- Related Changes When Upgrading to FastIron 08.0.95 or Later

The following table offers details regarding an upgrade to a FastIron 08.0.95 or later image with respect to ACLs.

TABLE 10 ACL-Related Upgrade Details

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
ACL MIB	• ACL MIBs are indexed using ACL ID. • Supported MIBs for ACLs bound to VE and interfaces only.	• ACL MIBs are indexed using ACL name. • MIB support for ACLs bound to VLAN, LAG, and VPORT (VLAN + port). • MIB is not supported for ACLs on VE. • You must switch to new ACL MIBs for RUCKUS ICX devices running FastIron 08.0.95 and later releases.

TABLE 10 ACL-Related Upgrade Details (continued)

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
IPv4 ACL filter	A number of well-known protocol name options are supported. A number of well-known TCP or UDP port name options are supported.	Well-known protocol name options of an IPv4 Extended ACL filter configuration are reduced to a few commonly used names. However, any protocol configuration is allowed by specifying the corresponding protocol number. TCP or UDP application port name options of an IPv4 Extended ACL filter configuration are reduced to a few commonly used application port names. However, any application can be configured by specifying the corresponding port number.
IPv6 ACL filter	A number of well-known protocol name options are supported. A number of well-known TCP or UDP port name options are supported.	Well-known protocol name options of an IPv6 ACL filter configuration are reduced to a few commonly used names. However, any protocol configuration is allowed by specifying the corresponding protocol number. TCP or UDP application port name options while configuring an IPv6 ACL filter are reduced to a few commonly used application port names. However, any application can be configured by specifying the corresponding port number.
MAC filter configuration	MAC filter configuration using the **mac filter** command is supported.	The MAC filter group configuration is auto-converted to a named MAC ACL in FastIron 08.0.95. The ACL logging or mirroring or accounting configuration in the MAC filter is migrated seamlessly. The **mac filter** command at the global level and the **mac filter-group** command at the interface level are deprecated and replaced by the **mac access-list** command with underlying filter statements beginning in FastIron 08.0.95. The accounting configuration for MAC filters that are not bound to any interface will be lost during upgrade and must be configured again for any resulting MAC ACL.
IPv4 ACL binding	The following configurations are supported in FastIron 08.0.92: • ACL binding at the VE level in a router image. • The per-VLAN ACL configuration in a switch image. • ACL binding at the selective port of a VE in a router image.	ACL binding to a VLAN on both the switch and router image is supported. The ACL binding configuration at the VE level is converted to a VLAN configuration. The ACL binding on the per-VLAN and selective port of a VE is converted to the binding of a selective port in a VLAN.
IPv6 ACL binding	ACL binding at the VE level in a router image is supported.	The binding of an ACL to a VLAN in both the switch and router image is supported. The ACL binding configuration at the VE level is converted to a VLAN configuration. Beginning with FastIron 08.0.95, the binding command **ipv6 traffic-filter** is changed to the **ipv6 access-group** command.
MAC filter binding	MAC filter binding is supported.	The MAC filter binding group forms a MAC ACL and is bound to an interface, much like an IP ACL. The MAC filter functionality remains intact. Beginning with FastIron 08.0.95, the **mac-filter group** command is modified to the **mac access-group** command.

TABLE 10 ACL-Related Upgrade Details (continued)

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
ACL Accounting	Accounting is enabled at the ACL level for IPv4 and IPv6 ACLs, and enabled at the filter level for MAC ACLs.	Accounting is configurable at an ACL level. Accounting is applied for all the filters on all interfaces to which the ACL is bound. ACL accounting is enabled by default. The **enable accounting** command has been introduced. The auto-migration uses the new **enable accounting** command.
ACL Logging	Logging is enabled at the interface level for IPv4 ACLs and at the ACL level for IPv6 ACLs, and enabled at the filter and filter-group level for MAC ACLs.	Logging is configurable only at the binding level using the **logging enable** command in conjunction with the **log** keyword at the filter level for IPv4, IPv6, and MAC ACLs. If ACL logging is enabled in an earlier release, ACL logging is enabled automatically under the resulting ACL binding after the upgrade process.
DSCP or PCP Remarking	The DSCP or PCP remarking configuration at the global level is supported.	In FastIron 08.0.95 and later releases, the DSCP or PCP remarking configuration at the global level is not supported, even though it was configured in a previous release. You can configure DSCP or PCP at the interface level, where DSCP actions will be merged with the user ACLs bound on the interface.
Per-port-per-VLAN	The per-port-per-VLAN configuration is supported.	The **enable acl-per-port-per-vlan** command is deprecated in FastIron 08.0.95. By default, all ports are enabled with per-port-per-VLAN.
ACL Policy	The **acl-policy** command and the **suppress-acl-seq** commands are supported. These commands are used during the downgrade process to FastIron 08.0.50 or releases prior to FastIron 08.0.50.	The **acl-policy** command and **suppress-acl-seq** commands are deprecated in FastIron 08.0.95.
ACL on ARP	ACL ID is not mandatory.	In FastIron 08.0.95 and later releases, an ACL ID is mandatory to configure an ACL on ARP. Enter an ACL number to specify the ACL to be used for filtering. If you have configured an ACL ARP without an ACL ID in an earlier release, the system will lose the configuration during the upgrade process.
ND-packet hop-limit check	The ND hop-limit configuration is configured using the **enable nd hop-limit** command under IPv6 ACL.	The ND hop-limit functionality is enabled by default. The **ipv6 nd ra-hop-limit** and **enable nd hop-limit** commands are deprecated. Checking for ND packets with a hop limit less than 255 helps protect against Denial of Service (DoS) attacks. The **enable nd hop-limit** command is deprecated beginning with FastIron 08.0.95.
Traffic Policy	The **cir** keyword of the traffic-policy rate-limit adaptive and traffic-policy rate-limit fixed commands is not supported in the configuration.	The **traffic-policy rate-limit adaptive** and **traffic-policy rate-limit fixed** commands are modified to add a new **cir** keyword. The rate can be specified as either packets or bytes.
DDoS	DDoS configuration on a virtual Ethernet interface is supported.	DDoS configuration at the VLAN level in a router image is allowed. During the upgrade process, the DDoS configuration at the VE level in a router image is applied to the VLAN in FastIron 08.0.95 and later releases.
DDoS configuration on a tagged or dual mode interface in a switch image	DDoS configuration is supported on a virtual Ethernet interface on router images and on tagged or dual mode interfaces in a switch image in releases prior to FastIron 08.0.95.	During the upgrade process, DDoS configuration under tagged or dual mode interface in a switch image will be lost. You must configure the same configuration under the VLAN in switch images in FastIron 08.0.95 and later.
DHCPv4 and DHCPv6 snooping on VLANs of a VLAN group	DHCPv4 or DHCPv6 snooping must be enabled on all the VLANs in a VLAN group.	DHCPv4 and DHCPv6 snooping on VLANs of a VLAN group is not supported. You will lose the configuration during the upgrade process.

TABLE 10 ACL-Related Upgrade Details (continued)

Functionality	FastIron 08.0.92	FastIron 08.0.95 or Later
IP Source Guard (IPSG)	IPSG configuration at the VE level in a router image, and at per-port-per-VLAN in a switch image is supported.	IPSG configuration at the VE level and at per-port-per-VLAN will be migrated to a VLAN with the selective port option.
IPSG and ingress IPv4 User ACL (UACL) for the same port	IPSG and ingress IPv4 UACL configuration for the same port can be configured together at the interface level or at the VE level or per-VLAN level.	If a port has both IPSG and UACL configuration together at any level, the upgrade process does not take place, and you will lose the UACL configuration. A warning message is displayed for the problem during bootup in FastIron 08.0.95 and later.
System default values and **system-max** commands for Static DAI and DHCP snooping	The system default value for Static Dynamic ARP Inspection (DAI) entries is 512 and for DHCP snooping is 8192. However, these default values can be changed for Static DAI and DHCP snooping using the **system-max max static-inspect-arp-entries** and **system-max max max-dhcp-snoop-entries** commands, respectively.	The **system-max** commands for Static DAI and DHCP snooping are deprecated beginning in FastIron 08.0.95, and the configurations are lost during the upgrade process. The new system default value for Static DAI is 6000 and for DHCP snooping is 32768.
DHCP snooping flash update interval configuration	The **ip dhcp snooping flash-update-interval** command is supported.	The **ip dhcp snooping flash-update-interval** command is deprecated beginning in FastIron 08.0.95 and the system will lose the configuration during the upgrade process.
System default values	The system default value depends upon the hardware.	The system default value depends upon the hardware. System default values for the ICX 7550 include the following values: • Maximum configurable filters the device supports (IPv4 and IPv6 ACLs): 8192 • Maximum configurable filters per ACL (either IPv4 or IPv6 ACLs): 2048 • MAC filter statements per ACL: 256 • MAC filter statements per stack: 3072
Authentication filter	MAC filter ID can be passed to the **authentication auth-filter** command configured in interface configuration mode.	The **authentication auth-filter** command is deprecated and replaced by the **authentication filter** command. A MAC ACL filter must be provided to this command instead of MAC ACLs. The MAC ACL filter supports source MAC address filters only.
Maximum VLAN support with User ACL (UACL) clients	There is no limit.	FastIron 08.0.95 and later releases support up to 512 VLANs to bind different clients having the same functionality. For example, features such as IPSG, DAI, and DHCP snooping can be enabled on 512 VLANs. A functionality enabled on more than 512 VLANs will lose the configuration during migration.
DHCP snooping or DAI or IPv6 Network Interface Identifier enabled on VLAN	DHCP snooping or DAI or Network Interface Identifier enabled on a VLAN without ports does not allocate hardware resources.	DHCP snooping or DAI or Network Interface Identifier enabled on a VLAN without ports allocates hardware resources for each VLAN for each Control Bridge (CB) unit. If TCAM space is full, enabling DHCP snooping or DAI or Network Interface Identifier on a VLAN without ports causes functionality failures during migration.
DHCP snooping database	The DHCP snooping database file name format is dhcpsnoop.db.	The DHCP snooping database file name format is icx_dhcp_snoop.db. Remove all entries from the DHCP binding database using the **clear dhcp** and **clear ipv6 dhcp6 snoop** commands before the downgrade process to a release prior to FastIron 08.0.95.

NOTE

On an ICX 7850 device, if you migrate to FastIron 08.0.95 or a later from a FastIron 08.0.92 configuration that contains an IPv4 egress ACL applied to a virtual interface, the two TCAM rules originally programmed for the ACL (one ACL rule and one implicit deny rule) are programmed as four TCAM rules in the target release configuration, where the ACL will be applied at the VLAN level; that is, two rules for the ACL and two rules for the implicit deny rule.

On an ICX 7850 device, if you migrate from FastIron 08.0.92 to FastIron 08.0.95 or a later, the rules created for an IPv6 egress ACL applied to a virtual interface multiply. For example, if you created the original IPv6 egress ACL with one rule, the ACL is programmed as four rules in TCAM for the FastIron 08.0.92 configuration; that is, one IPv6 ACL rule and three implicit rules. In the resulting configuration for the target release, the IPv6 ACL is applied at the VLAN level, and a total of eight rules will be created in TCAM; that is, two ACL rules and six implicit rules.

Upgrade Considerations for Stacks

ATTENTION

Before upgrading a stack from a release prior to FastIron 08.0.90 to FastIron 08.0.90 or later or downgrading from FastIron 08.0.90 or later to a release prior to FastIron 08.0.90, read this entire section.

Certain stack configuration behaviors have changed in FastIron 08.0.90, and new commands have been introduced to assist with upgrades and downgrades. For additional information on stacking changes, refer to the *RUCKUS FastIron Stacking Configuration Guide*.

Changes to Upgrade for Stacking from FastIron 08.0.90

The stacking port format is different beginning with FastIron 08.0.90. The change in format creates upgrade issues.

Upgrading a Stack to FastIron 08.0.90 or Later from Earlier Releases

Upgrades from earlier releases to FastIron 08.0.90 or later are seamless. FastIron 08.0.90 and later recognize the old format and parse the startup-config flash to convert the configuration to the new format. After upgrade, if you enter the **write memory** command to save the configuration, the new format is stored to the startup-config flash.

In the following example, an ICX 7550 stack is upgraded to FastIron 08.0.90 from the FastIron 08.0.80 startup-config flash. The user has not yet used the **write memory** command. Output for the **show configuration** command shows that the FastIron 08.0.80 startup-config flash remains in the old format. The command output for the **show running-config** command displays the runtime configuration in the new format.

```
ICX7550-48P Router# show configuration
!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 10.0.00_b255T243
!
stack unit 4
  module 1 icx7550-48-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 4/2/1
  stack-port ethernet 4/2/2
stack unit 5
  module 1 icx7550-48p-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 5/2/1
  stack-port ethernet 5/2/2
stack unit 6
```

```
  module 1 icx7550-48p-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 6/2/1
  stack-port ethernet 6/2/2
stack enable
stack rconsole-off
stack mac 8c7a.153f.1344
!
hitless-failover enable

====================================

ICX7550-48P Router# show running-config
Current configuration:
!
ver 09.0.10dT243
!
stack unit 4
  module 1 icx7550-48-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 4/2/1
  stack-port ethernet 4/2/2
stack unit 5
  module 1 icx7550-48p-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 5/2/1
  stack-port ethernet 5/2/2
stack unit 6
  module 1 icx7550-48p-port-management-module
  module 2 icx7550-qsfp-2port-80g-module
  module 3 icx7600-qsfp-2port-80g-module
  stack-port ethernet 6/2/1
  stack-port ethernet 6/2/2
stack enable
stack rconsole-off
stack mac 8c7a.153f.1344
!
hitless-failover enable
!
```

Downgrading a Stack to a Release Prior to FastIron 09.0.10a

NOTE

RUCKUS recommends that you establish a console connection with all stack units prior to the downgrade.

The major format change for stacking in the FastIron 09.0.10a is the inclusion of the **ethernet** keyword before port IDs (for example, **stack-port ethernet 1/2/1**) in the **stack-port**, **stack-trunk**, **multi-stack-port**, and **multi-stack-trunk** commands.

To downgrade to a release prior to FastIron 09.0.00 in the 08.0.9x format, copy the old startup-config file you saved previously back to the ICX device. The following example downgrades an ICX 7550 device by copying the file named saved_startup_08095 from the server at the specified IP address and saving it as startup-config.

```
ICX7550-48ZP Router# copy tftp startup-config 10.176.131.99 saved_startup_08095
Parameter Validation Successful
Startup Config Download started
Startup Config Download Done
Startup Config sync complete
Startup Config Write Done
Startup Config Download Complete
```

If you have backed up the configuration and you use the correct saved startup-config file, the stack will remain intact. However, if the stack breaks for any reason, such as a power failure, use the recovery procedure (Recovering a Broken Stack After a Downgrade from FastIron 09.0.10a or Later on page 34) to re-establish the stack and stacking connections.

If necessary, contact the Support Team for support. Refer to Contacting RUCKUS Customer Services and Support on page 5 for contact information and details on opening a ticket.

Recovering a Broken Stack After a Downgrade from FastIron 09.0.10a or Later

Downgrading from FastIron 09.0.10a or a later release is complex and may produce unexpected results. Refer to Downgrading a Stack to a Release Prior to FastIron 09.0.10a on page 33 for recommended steps before downgrading.

If a stack has broken following a downgrade from a more recent release to a FastIron 08.0.9x release, you can use the following procedure to recover the stack.

When the stack breaks on downgrade, the stack boots up without stack ports, as shown in the following example.

```
ICX7550-48 Router# show running-config
Current configuration:
!
ver 08.0.95c
!
stack unit 1
 module 1 icx7550-48-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 priority 128
stack unit 2
 module 1 icx7550-48-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 module 3 icx7600-xgf-4port-40g-module
stack unit 3
 module 1 icx7550-48p-port-management-module
 module 2 icx7550-qsfp-2port-80g-module
 module 3 icx7600-xgf-4port-40g-module
stack mac 4cb1.cd20.36be
```

NOTE
Depending on the target downgrade release, the **show running-config** command output may show different results. In some releases, default stack-ports may be present.

Complete the following steps to recover the stack.

1. Connect to the local console of the active controller.
2. In privileged EXEC mode, enter the **configure terminal** command.

```
ICX7550-48 Router# configure terminal
```

3. In global configuration mode, enter the **stack unit** command followed by the unit ID of the active controller (1 in the following example).

```
ICX7550-48 Router(config)# stack unit 1
```

4. Configure the original stack-ports or stack-trunks for the active controller.

   In the following example, two stack-ports are configured.

   ```
   ICX7550-48 Router(config-unit-1)# stack-port 1/2/1
   ICX7550-48 Router(config-unit-1)# stack-port 1/2/2
   ```

   NOTE
   You do not need to update the stack-ports or stack-trunks for the other stack units. The active controller learns the connections from the members as they join the stack.

5. Return to global configuration mode, and enter the **stack enable** command.

   ```
   ICX7550-48 Router(config-unit-1)# exit
   ICX7550-48 Router(config)# stack enable
   ```

   As soon as stacking is enabled, the active controller attempts to form a stack. However, the original standby controller may not join the stack because it may have become a standalone unit.

6. Use one of the following options to recover the standby controller:
   - Access the local console of the standby controller, and configure the original stack-ports or stack-trunks of the unit.
   - From the active controller, enter the **stack interactive-setup** command, and choose Option **3** when prompted to discover the standby unit as part of the stack.

     ```
     ICX7550-48 Router(config)# exit
     ICX7550-48 Router# stack interactive-setup
     You can abort stack interactive-setup at any stage by <ctrl-c>
     0: quit
     1: change stack unit IDs
     2: discover and convert new units (no startup-config flash) to members
     3: discover and convert existing/new standalone units to members
     2&3 can also find new links and auto-trunk or convert chain(s) to ring.

     Please type your selection: 3
     Probing topology to find standalone units...
     ```

7. Once the stack forms, enter the **write memory** command to save the running configuration.

Upgrade Process

NOTE
Before upgrading the software on a RUCKUS ICX device, refer to General Considerations for Upgrade to FastIron Release 10.0.00 or Later on page 12, General Considerations for Upgrade to FastIron Release 09.0.10a or Later on page 22, Initial Steps on page 23, and other relevant considerations included in this chapter. For a stacking system, also refer to Changes to Upgrade for Stacking from FastIron 08.0.90 on page 32.

Software images for all RUCKUS ICX devices can be uploaded and downloaded between flash modules on the device and a TFTP, SCP, HTTPS, or USB module on the network.

RUCKUS ICX devices have two flash memory modules:

- Primary flash: The default local storage device for image files and configuration files.
- Secondary flash: A second flash storage device. You can use secondary flash to store redundant images for additional booting reliability or to preserve one software image while testing another one.

Only one flash device is active at a time. By default, the primary image becomes active when you reboot the device.

The following methods are available to upgrade your RUCKUS ICX device:

- Trivial File Transfer Protocol (TFTP): Use TFTP to copy an image from a TFTP server onto a flash module.
- Secure Copy Protocol (SCP): Use SCP to copy images to and from a host (recommended).
- Hypertext Transfer Protocol Secure (HTTPS): Beginning with FastIron 08.0.80, you can use HTTPS, which requires a server that supports HTTP over TLS.
- Universal Serial Bus (USB): Use a USB device that contains the appropriate files and is connected to a standalone unit or the active controller in a stack.

Mandatory Upgrade Steps from a Pre-08.0.80 Non-UFI Version to a 09.0.10a or Later UFI Version

Upgrading from a pre-08.0.80 non-UFI version to a FastIron 09.0.10a or later UFI version is a two-step upgrade process. For example, if you want to upgrade a stacking unit or a standalone device from FastIron 08.0.70 to FastIron 09.0.10a or later, complete the following steps.

1. Download the 08.0.80f non-UFI using one of the transfer methods listed in Table 11, and reboot the device with the FastIron 08.0.80f image using the **boot system flash primary** command. The system uses the FastIron 08.0.80f image. Save the running configuration to the startup configuration using the **write memory** command.

   NOTE
   Downloading the non-UFI image and rebooting the device is mandatory because it migrates the configured access control list (ACL) configurations without sequence numbers to the new ACL format. The system will otherwise lose the previously configured ACL configuration without sequence numbers while upgrading from a pre-08.0.90 non-UFI version to a UFI version.

2. Copy the FastIron 09.0.10a or later UFI to the primary flash partition using the same method, and reboot the device again.

   NOTE
   The **show version** command may display a boot code mismatch message after the upgrade.

   Copy the FastIron 09.0.10a or later UFI again to the secondary flash partition to avoid boot image mismatch.

   NOTE
   You must download the FastIron 08.0.95 image using one of the transfer methods listed in Table 11 to upgrade a device from FastIron 08.0.80 to FastIron 09.0.10a.

TABLE 11 File Transfer Method and Commands Required for Upgrading from Pre-08.0.80 Non-UFI Version

Transfer Method	Commands
TFTP	1a) device# copy tftp flash 10.177.16.144 SPR08080f.bin primary 1b) device# copy tftp flash 10.177.16.144 spz10114.bin bootrom 2a) device# copy tftp flash 10.177.16.144 SPR09010aufi.bin primary 2b) device# copy tftp flash 10.177.16.144 SPR09010aufi.bin secondary or 1) device# copy tftp system-manifest 10.176.220.51 FI08080f_Manifest.txt all-images-primary 2a) device# copy tftp system-manifest 10.176.220.51 FI09010a_Manifest.txt primary 2b) device# copy tftp system-manifest 10.176.220.51 FI09010a_Manifest.txt secondary

TABLE 11 File Transfer Method and Commands Required for Upgrading from Pre-08.0.80 Non-UFI Version (continued)

Transfer Method	Commands
SCP	1a) device# copy scp flash 10.176.132.13 SPR08080f.bin primary 1b) device# copy scp flash 10.176.132.13 spz10114.bin bootrom 2a) device# copy scp flash 10.176.132.13 SPR09010aufi.bin primary 2b) device# copy scp flash 10.176.132.13 SPR09010aufi.bin secondary
HTTPS (FastIron 08.0.80 and later)	1a) device# copy https flash 10.176.132.132 SPR08080f.bin primary 1b) device# copy https flash 10.176.132.132 spz10114.bin bootrom 2a) device# copy https flash 10.176.132.132 SPR09010aufi.bin primary 2b) device# copy https flash 10.176.132.132 SPR09010aufi.bin secondary
USB	1a) device# copy disk0 flash SPR08080f.bin primary 1b) device# copy disk0 flash spz10114.bin bootrom 2a) device# copy disk0 flash SPR09010aufi.bin primary 2b) device# copy disk0 flash SPR09010aufi.bin secondary

NOTE

The system will lose the auth-filter configuration during the upgrade process to FastIron 09.0.10a or later or upon a reload with a FastIron 08.0.80 release. You must reconfigure the **authentication-filter** command after the system reloads with the FastIron 09.0.10a or later image.

Loading the Flash Code Using TFTP

NOTE

For ICX7550 or ICX 7650 (running FastIron 08.0.80a and later) or ICX 7850, proceed to step 2.

1. Copy the 08.0.80f non-UFI from the TFTP server into flash memory using the **copy tftp flash** command.

```
ICX7650-48 Router# copy tftp flash 10.177.16.144 SPR08080f.bin primary
Load to buffer (8192 bytes per dot)
.....................................................................
.....................................................................
TFTP to Flash Done.
```

a) Copy the bootrom images using the following command.

```
ICX7650-48 Router# copy tftp flash 10.177.16.144 spz10114.bin bootrom
Load to buffer (8192 bytes per dot)
.....................
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
............
TFTP to Flash Done.
```

b) Enter the **show flash** command to verify the image and uboot files have been installed in the primary partition flash.

```
ICX7650-48 Router# show flash
Stack unit 1:
  Compressed Pri Code size = 29829112, Version:08.0.80fT213 (SPR08080f.bin)
  Compressed Sec Code size = 29515932, Version:08.0.70fT213 (SPR08070f.bin)
  Compressed Boot-Monitor Image size = 786432, Version:10.1.14T215
  Code Flash Free Space = 1613783040
```

c) Reboot the device with the 08.0.80f image using the **boot system** command.

NOTE

Use the **boot system flash primary** command to boot the image from the primary flash memory.

```
ICX7650-48 Router# boot system flash primary
```

d) Enter the **show version** command to display the flash image running on the device.

```
ICX7650-48 Router# show version
Copyright (c) 2017 Ruckus Wireless, Inc. All rights reserved.
    UNIT 1: compiled on Apr  6 2020 at 22:40:21 labeled as SPR08080f
      (29829112 bytes) from Primary SPR08080f.bin
        SW: Version 08.0.80fT213
      Compressed Boot-Monitor Image size = 786944, Version:10.1.14T215 (spz10114)
       Compiled on Thu Nov 15 12:59:16 2018

  HW: Stackable ICX7650-48
==========================================================================
UNIT 1: SL 1: ICX7650-48 48-port Management Module
      Serial  #:DUJ3851L0CL
      Software Package: ICX7250_L3_SOFT_PACKAGE   (LID: fwlINKGnFen)
      Current License: l3-prem-8X10G
      P-ASIC  0: type B344, rev 01  Chip BCM56344_A0
==========================================================================
UNIT 1: SL 2: ICX7250-SFP-Plus 8-port 80G Module
==========================================================================
1000 MHz ARM processor ARMv7 88 MHz bus
8192 KB boot flash memory
2048 MB code flash memory
2048 MB DRAM
STACKID 1  system uptime is 2 minute(s) 41 second(s)
The system started at 04:27:55 GMT+00 Wed Jul 29 2020

The system : started=warm start   reloaded=by "reload"
```

2. Copy the 09.0.10a or later UFI from the TFTP server into flash memory using the **copy tftp flash** command.

```
ICX7650-48 Router# copy tftp flash 10.177.16.144 SPR09010aufi.bin primary

Load to buffer (8192 bytes per dot)
.....................................................
.....................................................
Processing the bundle image...
Flashing application image to Primary partition...

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
.....................................................
Flashing bootrom image...

SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(65536 bytes per dot)...
............
Post processing bundle image...
Bundle image processed successfully
```

a) Save the running configuration to startup configuration using the **write memory** command.

```
ICX7650-48 Router# write memory
```

b) Reboot the device with the 09.0.10a or later UFI image using the **boot system flash primary** command.

```
ICX7650-48 Router# boot system flash primary
```

NOTE

The system does not support full functionality such as third-party packages (DHCPv6, HTTP, Python, and so on.) without a UFI update. If you stop the upgrade process after the reboot without downloading the UFI, the following warning message is displayed on the console.

```
WARNING: FI image is not booted from UFI. Please download UFI image and reboot the
system for
 full functionality.
```

NOTE

The **show version** command might display boot code mismatch message after performing the above upgrade.

c) Re-copy the 09.0.10a or later UFI from the TFTP to the secondary flash partition to avoid boot image mismatch.

```
ICX7650-48 Router# copy tftp flash 10.176.198.42 SPR09010aufi.bin secondary
Parameter Validation Successful
Image Download started

SYSLOG: <14> Sep 30 20:31:48 ICX7650-48 Router COPY IMAGE TO FLASH START
.................................................Image Download Done
Image Validation Started

SYSLOG: <14> Sep 30 20:33:05 ICX7650-48 Router COPY APPLICATION IMAGE FROM BUNDLE START

SYSLOG: <14> Sep 30 20:33:05 ICX7650-48 Router COPY BOOTROM IMAGE FROM BUNDLE START
Image Write Done
Image Download Complete
ICX7650-48 Router#
SYSLOG: <14> Sep 30 20:33:25 ICX7650-48 Router COPY BUNDLE IMAGE COMPLETED
```

d) Enter the **show version** command to display the flash image running on the device.

```
ICX7650-48 Router# show version

Copyright (c) Ruckus Networks, Inc. All rights reserved.
    UNIT 1: compiled on Jul 20 2021 at 22:56:24 labeled as SPR09010a
      (32947884 bytes) from Primary SPR09010a.bin (UFI)
        SW: Version 09010a
      Compressed Primary Boot Code size = 786944, Version:10.1.18T215 (spz10118)
```

```
       Compiled on Mon Jul 13 08:53:15 2021

  HW: Stackable ICX7650-48
==========================================================================
UNIT 1: SL 1: ICX7650-48 48-port Management Module
      Serial  #:DUJ3851L0CL
      Software Package: ICX7250_L3_SOFT_PACKAGE   (LID: fwlINKGnFen)
      Current License: l3-prem-8X10G
      P-ASIC  0: type B344, rev 01  Chip BCM56344_A0
==========================================================================
UNIT 1: SL 2: ICX7250-SFP-Plus 8-port 80G Module
==========================================================================
1000 MHz ARM processor ARMv7 88 MHz bus
    8 MB boot flash memory
    2 GB code flash memory
    2 GB DRAM
STACKID 1  system uptime is 1 minute(s) 49 second(s)
The system started at 04:41:32 GMT+00 Wed Jul 29 2021

The system : started=warm start   reloaded=by "reload"
```

e) Enter the **show flash** command to verify the image and uboot files.

```
ICX7650-48 Router# show flash
Stack unit 1:
  Compressed Pri Code size = 33554432, Version:09.0.10aT213 (SPR09010a.bin)
  Compressed Sec Code size = 33554432, Version:09.0.10aT213 (SPR09010a.bin)
  Compressed Pri Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Compressed Sec Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Code Flash Free Space = 1492922368
Stack unit 2:
  Compressed Pri Code size = 33554432, Version:09.0.10aT213 (SPR09010a.bin)
  Compressed Sec Code size = 33554432, Version:09.0.10aT213 (SPR09010a.bin)
  Compressed Pri Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Compressed Sec Boot Code size = 786944, Version:10.1.20T215 (spz10120b35)
  Code Flash Free Space = 1496690688
ICX7650-48 Router#
```

When upgrading the flash image version, the image is automatically updated across all stack units. When upgrading from one major release to another (for example, from FastIron 08.0.90 to FastIron 09.0.10a), make sure that every unit in the traditional stack has the same major code version. If you reboot the stack while units are running different code versions, the units cannot communicate.

Loading the Flash Code Using SCP

The new flash code must be placed on an SCP-enabled host to which the RUCKUS ICX device has access.

NOTE
Copying the manifest file using SCP is not supported.

NOTE
The FastIron CLI must be used for the SCP image copy.

1. Copy the flash code from the SCP-enabled host into flash memory.

```
ICX7550-24P Router# copy scp flash 10.176.132.13 GZR09010dufi.bin primary

User name:root
Password:
Connecting to remote host......

Receiving data (8192 bytes per dot)
.................................
Automatic copy to member units:  1  4
SYNCING IMAGE TO FLASH. DO NOT SWITCH OVER OR POWER DOWN THE UNIT(8192 bytes per dot)...
Image copy completed
Primary Image file downloaded successfully.
SCP transfer to device completed
Outbound Connection Closed
```

   a) Save the running configuration to the startup configuration using the **write memory** command.

```
ICX7550-24P Router# write memory
```

2. Reload the device and then immediately upgrade to the UFI.

```
ICX7550-24P Router# boot system flash primary
```

   a) Copy the 09.0.10a or later UFI again to the primary and the secondary flash partitions to avoid boot image mismatch.

```
ICX7550-24P Router# copy scp flash 10.176.132.13 GZR09010dufi.bin primary
User name:root
Password:
Connecting to remote host......

Receiving data (8192 bytes per dot)
Image copy completed

ICX7550-24P Router# copy scp flash 10.176.132.13 GZR09010dufi.bin secondary
```

Loading the Flash Code Using HTTPS

1. Copy the flash code from HTTPS to flash memory.

```
ICX7550-48P Router# copy https flash 10.176.132.132 GZR09010dufi.bin primary
```

   a) Save the running configuration to the startup configuration using the **write memory** command.

```
ICX7550-48P Router# write memory
```

2. Reload the device and then immediately upgrade to the UFI.

```
ICX7550-48P Router# boot system flash primary
```

   a) Copy the FastIron 09.0.10a or later UFI again to the primary and the secondary flash partitions to avoid boot image mismatch.

```
ICX7550-48P Router# copy https flash 10.176.132.132 GZR09010dufi.bin primary
ICX7550-48P Router# copy https flash 10.176.132.132 GZR09010dufi.bin secondary
```

Loading the Flash Code Using a USB Device

1. a. Copy the application image and the boot image to the flash memory from the USB device.

```
ICX7550-48P Router# copy disk0 flash GZR09010dufi.bin primary
```

a) Save the running configuration to the startup configuration using the **write memory** command.

```
ICX7550-48P Router# write memory
```

2. Reload the device and then immediately upgrade to the UFI.

```
ICX7550-48P Router# boot system flash primary
```

a) Copy the FastIron 09.0.10a or later UFI again to the primary and the secondary flash partitions to avoid boot image mismatch.

```
ICX7550-48P Router# copy disk0 flash GZR09010dufi.bin primary
ICX7550-48P Router# copy disk0 flash GZR09010dufi.bin secondary
```

b) Enter the **show version** command to verify that the UFI image has loaded successfully.

```
ICX7550-48P Router# show version
Copyright (c) Ruckus Networks, Inc. All rights reserved.
UNIT 5: compiled on Jul 4 2022 at 22:57:26 labeled as GZR09010d
(65658632 bytes) from Primary GZR09010d.bin (UFI)
SW: Version 09.0.10dT243
Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
Compiled on Thu Apr 21 11:22:29 2022
UNIT 4: compiled on Jul 4 2022 at 22:57:26 labeled as GZR09010d
(65658632 bytes) from Primary GZR09010d.bin (UFI)
SW: Version 09.0.10dT243
Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
UNIT 6: compiled on Jul 4 2022 at 22:57:26 labeled as GZR09010d
(65658632 bytes) from Primary GZR09010d.bin (UFI)
SW: Version 09.0.10dT243
Compressed Primary Boot Code size = 1081856, Version:10.1.25T245 (gzu10125)
HW: Stackable ICX7550-48-POE
==========================================================================
UNIT 4: SL 1: ICX7550-48 48-port Management Module
Serial #:FML4208R00Y
Software Package: ICX7550_BASE_L3_SOFT_PACKAGE
Current License:
==========================================================================
UNIT 4: SL 2: ICX7550-QSFP 2-port 80G Module
==========================================================================
UNIT 4: SL 3: ICX7600-2X40GQ 2-port 80G Module
Serial #:FMN4210R010
Software Package: ICX7550_L3_SOFT_PACKAGE
Current License: l3-prem
P-ASIC 8: type B371, rev 03 Chip BCM56371_A2
==========================================================================
UNIT 5: SL 2: ICX7550-QSFP 2-port 80G Module
==========================================================================
UNIT 5: SL 3: ICX7600-2X40GQ 2-port 80G Module
Serial #:EZG4207R004
==========================================================================
UNIT 6: SL 1: ICX7550-48P POE 48-port Management Module
Serial #:FMN4210R016
Software Package: ICX7550_BASE_L3_SOFT_PACKAGE
Current License: l3-base
==========================================================================
UNIT 6: SL 2: ICX7550-QSFP 2-port 80G Module
==========================================================================
UNIT 6: SL 3: ICX7600-2X40GQ 2-port 80G Module
Serial #:EZG4207R006
==========================================================================
1700 MHz ARMv8 Cortex-A72 processor 857 MHz bus
16 MB boot flash memory
4 GB code flash memory
4 GB DRAM
STACKID 5 system uptime is 18 hour(s) 51 minute(s) 9 second(s)
STACKID 4 system uptime is 18 hour(s) 51 minute(s) 12 second(s)
STACKID 6 system uptime is 18 hour(s) 51 minute(s) 8 second(s)
The system started at 03:50:31 GMT+00 Wed Jul 06 2022
The system : started=warm start reloaded=by "reload"
My stack unit ID = 5, bootup role = active
```

Upgrading from a UFI Version to a Later UFI Version

NOTE
Beginning with FastIron release 10.0.00, manifest file copy is no longer supported for the switch image (Layer 2). The router image (Layer 3) UFI must be used for the manifest file copy process to work correctly.

Upgrading from a UFI version to a later UFI version is a one-step upgrade process.

If you want to upgrade from a UFI version (for example, 08.0.92) to FastIron 09.0.10a or later, download the FastIron 09.0.10a or later UFI and use the **boot system flash primary** command to reload the device. Copy the FastIron 09.0.10a or later UFI again to the primary and secondary flash partitions to avoid boot image mismatch.

TABLE 12 File Transfer Method and Commands Required for Upgrading from a UFI Version

Transfer Method	Commands
TFTP	1a) device# copy tftp flash 10.176.132.11 TNR10000ufi.bin primary 1b) device# copy tftp flash 10.176.132.11 TNR10000ufi.bin secondary or 2a) device# copy tftp system-manifest 10.176.132.11 FI10000_Manifest.txt primary 2b) device# copy tftp system-manifest 10.176.132.11 FI10000_Manifest.txt secondary
SCP	device# copy scp flash 10.176.132.11 TNR10000ufi.bin primary device# copy scp flash 10.176.132.11 TNR10000ufi.bin secondary
HTTPS	device# copy https flash 10.176.132.132 TNR10000ufi.bin primary device# copy https flash 10.176.132.132 TNR10000ufi.bin secondary
USB	device# copy disk0 flash TNR10000ufi.bin primary device# copy disk0 flash TNR10000ufi.bin secondary

Using a USB Device for Image Download

Beginning with FastIron 08.0.90, the system can be upgraded by downloading the manifest file in the USB drive.

When TFTP server access is not available, you can use the manifest file in the USB drive to download the images of a system. Manifest image download using a USB device is not supported for FastIron 08.0.80 and earlier. In earlier releases, USB image download was supported for standalone systems only. USB image download is supported on all ICX devices.

Complete the following steps to initiate the upgrade using the USB drive.

1. Plug in a valid USB drive (USB2 drives and backward-compatible USB3 drives) with the appropriate pre-loaded manifest files to the system.
2. Reload the unit with the USB drive plugged in.

NOTE
USB image download is not supported in FIPS mode.

Software upgrade using a USB device is not triggered in the following scenarios:

- If the USB drive is not detected during the bootup.
- When the USB drive is corrupted, not accessible, unmountable, or if there is no valid file system in the USB drive.
- If there is an existing configuration file in the system.

NOTE
To delete an existing configuration file, the configuration file must be deleted from the system using the **erase startup-configuration** command. Image download using a USB device is not triggered if there is a configuration file in the system.

When the image is successfully copied and upgraded, the system automatically reloads. On bootup, the system copies the configuration file from the USB drive. Then the system reloads with the updated image and the new configuration. If there are multiple configuration files in the USB drive, the configuration files are copied in the following order (in descending priority):

- *model*.cfg (for example, ICX7650.cfg,"ICX7550.cfg)
- default.cfg

Upgrade Using the Manifest File in the USB Drive

Beginning with FastIron 08.0.90, the **copy disk0 system-manifest** command can be used to copy the manifest file from a USB device. The images stored in the USB disk are copied to the primary or secondary partition based on the choice of partition. This image can be an application image or a Unified FastIron Image (UFI).

If you are upgrading the system to FastIron 08.0.80 or later, the system will upgrade the images using UFI.

If you are downgrading the system to FastIron 08.0.70 or earlier, only the application image is supported.

NOTE
RUCKUS does not recommend non-UFI downgrades.

NOTE
After the USB image download, you must use the **unmount disk0** command before removing the disk.

After the manifest file is successfully downloaded, the manifest.txt file in the flash memory is retained for any future reverse manifest.

If the image is not successfully downloaded from the manifest file, the following warning message is displayed:

```
Possible failure on one of the member units while downloading the image. Images may not be in sync after
reloading.
```

You can upgrade a failed member unit. If you reload the system, an image mismatch occurs, and auto-copy upgrades the unit.

Auto-Download Using a USB Device

When the system boots up, it checks for a valid manifest file, and if the manifest file is available, the system begins copying the files from the USB drive to the system flash memory. The system copies the images only through manifest file download and picks only the image listed in the manifest file. The system also copies the signature file and boot image files listed by the manifest file. It is recommended that the USB drive contain only one manifest file set. If there are multiple manifest files in the USB drive, the system selects the first available manifest file (the order of the manifest files is not defined). The image and boot image in the USB drive must be of a different version than in the system flash memory.

In case of an image mismatch between control bridge and port extender images, the mismatched port extender images can be upgraded using a configured TFTP server.

Beginning with FastIron 08.0.90, the correct image stored in the USB drive is used to upgrade and reload the mismatched port extender images.

If the TFTP server does not have the correct image, the image in the USB drive is used. The correct image stored in the USB drive is used for the port extender. If the USB drive does not have the correct image, the port extender will remain in a mismatched state.

The USB status mode LED indicates the status of the bootup from USB drive.

Refer to the platform-specific hardware installation guide for more information.

Copying the UFI and Manifest Packages from System Flash to a USB Drive

Beginning with FastIron 09.0.10a, you can copy the UFI and manifest packages from system flash to a USB drive using the CLI. The same USB drive can be plugged-in to another system for copying the UFI and manifest packages. You can make a backup of the UFI or manifest packages to a USB drive before performing any upgrade process.

The USB status mode LED blinks green to show that the UFI or manifest copy is in progress. The LED turns to steady green once the copy is completed successfully. If the copy fails, either due to a flash read issue or USB access or write issue, the LED blinks amber to notify you of the failure. During the entire operation of the UFI or manifest copy, the flash will be locked to avoid any other flash operations.

If there is not enough file system space available in the USB drive, the following error message is displayed:

```
Not enough space on the filesystem to copy the source file.
```

While copying the manifest package from flash to the USB drive, the system copies the manifest file, UFI, UFI signature, and configuration files. Beginning with FastIron 09.0.10a, the manifest package contains only the UFI for all ICX devices.

Commands for Copying from Flash to a USB Device

To initiate the copy of UFI from flash to a USB drive using the CLI, use the following commands:

- **copy flash disk0 ufi-primary** *image-file:* Use this command to copy the UFI of the primary partition to the USB drive in the name as specified by *image-file*.
- **copy flash disk0 ufi-secondary** *image-file:*Use this command to copy the UFI of the secondary partition to the USB drive in the name as specified by *image-file*.
- Use the **copy flash disk0 system-manifest**: Use this command to copy the manifest package on the UFI of the current running partition and UFI signature to a USB drive.

Limitations

When one partition has a legacy image (for example, FastIron 08.0.70) and another partition has a UFI, copying the UFI and manifest package to a USB drive from a partition that has the legacy image is not supported.

If there is a flash corruption in the system, the configurations, logs, and the UFI will be lost. In such a case, copying the UFI and manifest package to a USB drive is not possible. However, you can copy the FastIron image to a USB drive using the **copy flash disk0** command because the partition for the FastIron image is different.

OS Prompt Recovery Procedures

> **NOTE**
> Beginning with FastIron 09.0.10a, the **no password** command is no longer supported at the uboot prompt. Refer to "Password and Device Recovery" in the *RUCKUS FastIron Management Configuration Guide* guide for information on password recovery.

If during an upgrade procedure, the ICX device enters the OS mode and does not exit, use the **copy tftp flash** command at the OS prompt to re-install the image.

The following example downloads the FastIron 09.0.10a UFI from the TFTP server at the specified IP address to primary flash memory in the ICX device.

```
OS> copy tftp flash 192.168.10.89 SPR9010aufi.bin primary
```

To configure the IP address, subnet mask, and default gateway for an ICX device in OS mode, use the **remote_address** and **remote_gateway** commands, as shown in the following example.

```
OS> remote_address 10.176.132.159 255.255.255.128
OS> remote_gateway 10.176.132.129
```

To copy the FastIron image from the remote TFTP server to the ICX device at the OS prompt, use the **copy tftp flash** command followed by the IP address of the server, the correct image name, and the target flash location (primary or secondary), as shown in the following example.

```
OS> copy tftp flash 10.176.198.42 SPR09010aufi.bin secondary
Copying SPR09010aufi.bin from 10.176.198.42
SPR09010aufi.bin     100% |*****************************|
```

Software Recovery

If a software upgrade or downgrade fails, the device may reboot continuously, as shown in the following CLI output.

```
bootdelay: ===
Booting image from Primary
Bad Magic Number
could not boot from primary, no valid image; trying to boot from secondary
Booting image from Secondary
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
could not boot from secondary, no valid image; trying to boot from primary
Booting image from Primary
Bad Magic Number
## Booting image at 01ffffc0 ...
Bad Magic Number
```

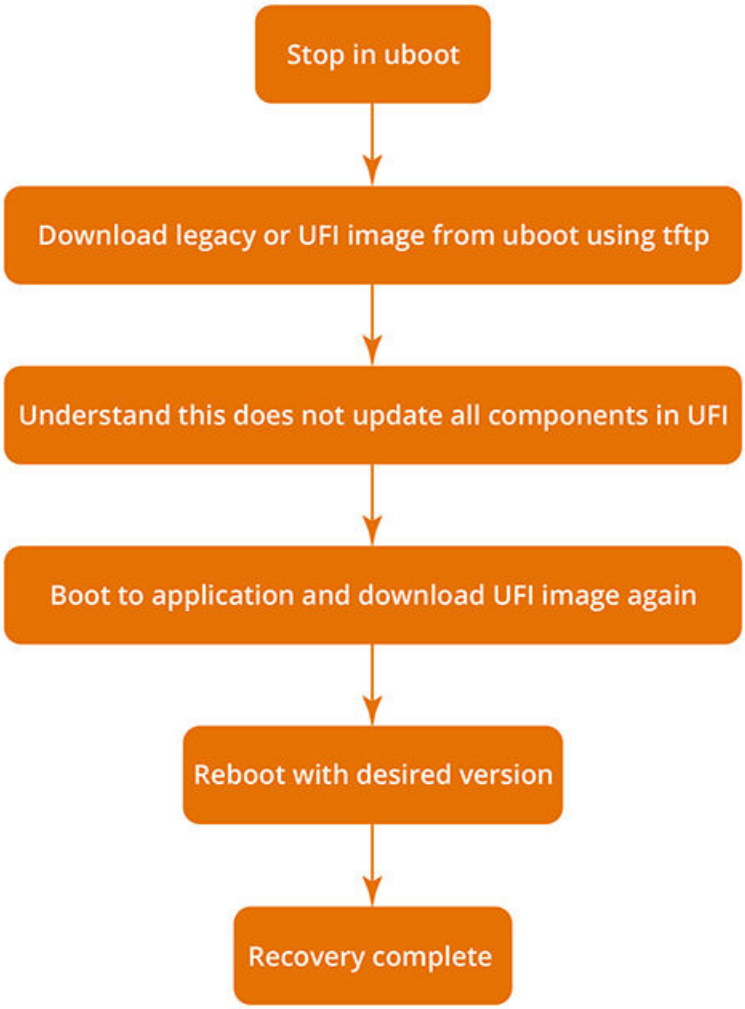
Recovering Software

Software recovery involves recovering devices from image installation failure or deleted or corrupted flash images.

NOTE
Software recovery should be performed under the supervision of a RUCKUS Support engineer.

NOTE
To stop at the uboot prompt from the console, continuously press **b** during the boot process.

FIGURE 1 Recovery Procedure



1. Connect a console cable from the console port to the terminal server.
2. Connect an Ethernet cable from the management port (the port located under the console port on the device) to the TFTP server.

   The device will be in boot mode for recovery.
3. Display the existing variables from the boot prompt.

```
ICX7550-Boot> printenv
baudrate=9600
ipaddr=10.176.134.154
serverip=10.176.195.200
netmask=255.255.255.128
gatewayip=10.176.134.129
uboot=mnz10120b35.bin
image_name=SPR08095d.bin
ver=10.1.20b35T225 (Apr 29 2021 - 23:48:55 -0700)
```

   The path is to the boot image on the TFTP server.

4. Use the **setenv serverip** command to set the TFTP server that hosts a valid ICX software image.

```
ICX7550-Boot> setenv serverip 10.10.10.21
```

5. Use the **setenv ipaddr** command to set the IP address, the **setenv gatewayip** command to set the gateway IP address, and the **setenv netmask** command to set the netmask for the device management port; and use the **saveenv** command to save the configuration.

```
ICX7550-Boot> setenv ipaddr 10.10.10.22
ICX7550-Boot> setenv gatewayip 10.10.10.1
ICX7550-Boot> setenv netmask 255.255.255.0
ICX7550-Boot> saveenv
```

NOTE
The IP address and the gateway IP address set for the device management port should be for the same subnet as the TFTP server NIC.

6. Enter the **print** command to verify the IP addresses that you configured for the device and the TFTP server.

```
ICX7550-Boot> print
baudrate=9600
boot_partition=pri_partition
bootcmd=run defbootcmd
bootdelay=5
console=ttyS0
crashkernel=crashkernel=104M
defbootcmd=usb start;setenv bootargs ip=${ipaddr}:${serverip}:${gatewayip}:${netmask}:${hostname}:$
{netdev}:off console=ttyS0,${baudrate},${extra_bootargs},${fips_reset},${fips_enabled} maxcpus=1 $
{crashkernel} ${softdog} ${debug} root=/dev/ram ethaddr=${ethaddr}? ${quiet} ${lnxdbg}
boot_partition=${boot_partition}; ext4load usb 0:1 0x64000000 ${image_to_boot}; bootm
0x64000200#conf_1
ethact=bcm_xgs_gmac-0
ethaddr=4c:b1:cd:20:2f:c5
fdt_high=0xffffffffffffffff
gatewayip=10.176.132.1
hostname=GODZILLA
image_to_boot=primary.bin
ipaddr=10.176.132.98
netdev=eth0
netmask=255.255.255.128
serverip=10.176.198.42
stderr=serial
stdin=serial
stdout=serial
uboot=gzu10125.bin
uboot_size=1572864
ver=10.1.25T245 (Jun 29 2022 - 05:53:39 -0700)
ver_red=10.1.25T245 (Jun 29 2022 - 05:53:39 -0700) Broadcom Helix 5

Environment size: 975/131068 bytes
ICX7550-Boot>
```

7. Use the **ping** command to test the connectivity to the TFTP server from the device to ensure a working connection.

```
ICX7550-Boot> ping 10.10.10.21
ethPortNo = 0
Using egiga0 device
host 10.10.10.21 is alive
```

8. Use the **setenv image_name** command to provide the file name of the image that you want to copy from the TFTP server.

```
ICX7550-Boot> setenv image_name GZR09010dufi.bin
```

9. Use the **update_primary** or **update_secondary** command as appropriate to update the flash memory.

```
ICX7550-Boot> update_primary
```

10. Use the **boot_primary** or **boot_secondary** command as appropriate to load the image from the primary or secondary flash memory.

```
ICX7550-Boot> boot_primary
```

In-Service Software Upgrade

- In-Service Software Upgrade Overview....51
- ISSU Limitations and Considerations....51
- Recommended Stack Topology for ISSU....51
- How ISSU Works When Upgrading Stack Units....52
- Upgrading a Stack with ISSU....54
- ISSU Errors....59
- Manual Error Recovery....60

In-Service Software Upgrade Overview

An in-service software upgrade (ISSU) allows stack units to be upgraded with minimal interruptions to multi-unit topologies.

ISSU provides an incremental method to upgrade traditional stacks. A successful ISSU does not affect uplink or downlink connectivity in a topology with multi-unit LAGs. Only the node that is undergoing the upgrade requires a hardware reset that includes the reset of the packet processor. As a result, traffic transiting only that node is disrupted.

ISSU Limitations and Considerations

When using ISSU, consider the following capabilities and restrictions:

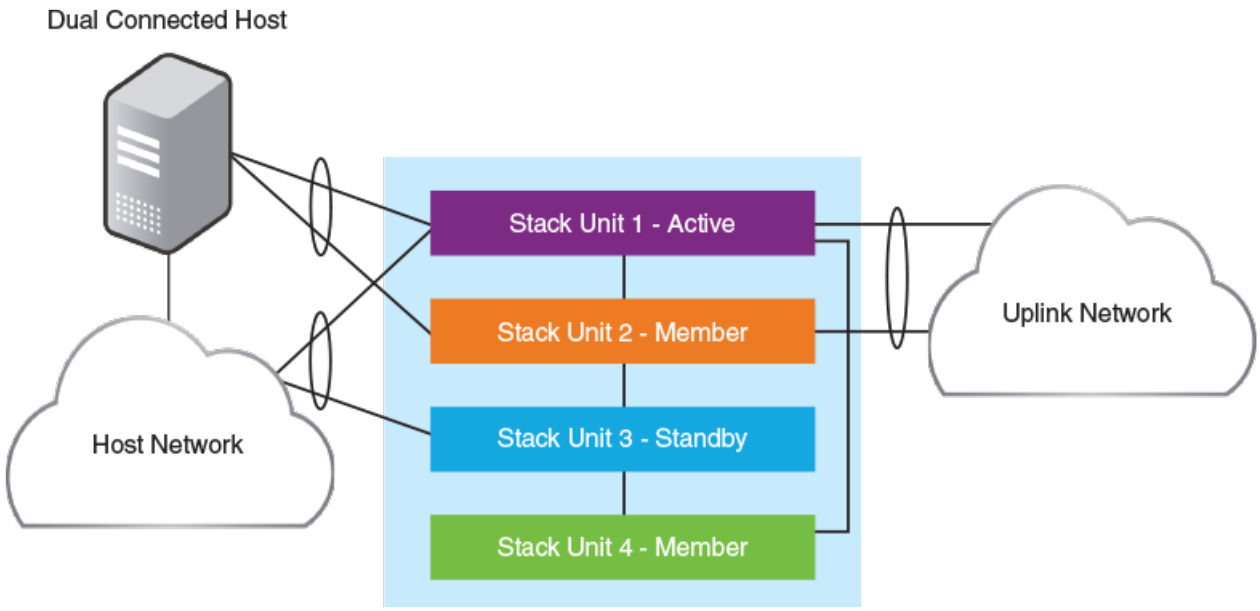
- ISSU is supported on FastIron stackable hardware.
- ISSU is supported in a traditional ring stack topology.
- ISSU works for stacks of two units to the maximum supported twelve units.
- ISSU is supported for upgrades between minor releases only. For example, you can use ISSU to upgrade between FastIron 08.0.90 and FastIron 08.0.90a or between FastIron 08.0.90a and subsequent patch releases, but not between FastIron 09.0.10a and FastIron 10.0.00.
- For ISSU to occur with minimal disruption, the customer network connected to the stack must have redundant uplink and downlink configurations across multiple units.
- If the secondary partition is upgraded, this secondary partition is set as the default boot partition for the stack.
- Most CLI commands, SNMP, and web operations are blocked while ISSU is in progress.
- To make the upgrade seamless, the following administrative operations are blocked while ISSU is in progress:
  - Configuration
  - Image download to flash memory
  - Stack commands that may result in topology change or discovery
  - Initiation of another ISSU

Recommended Stack Topology for ISSU

ISSU provides an ability to upgrade traditional stacks without affecting the network.

ISSU reduces its network impact only if redundant uplink and downlink connections are available from multiple stack units. A typical topology where ISSU can be used effectively is shown in the following figure.

FIGURE 2 Recommended Stack Topology for ISSU



In the figure, redundant links are going to both the uplink network and the downlink network from different units of the stack. At any point during the upgrade, the uplink and downlink connectivity is maintained. The following software features are used to provide link redundancy:

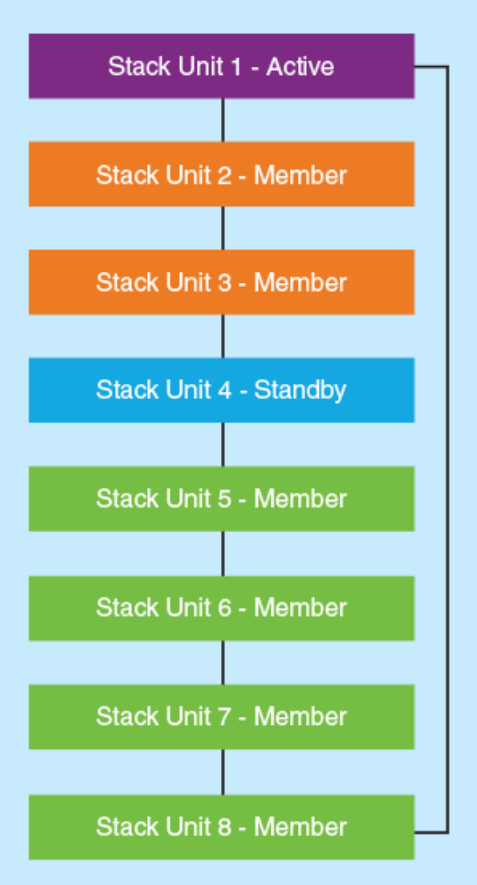
- Link aggregation (or dual connectivity to two different PEs in a chain or ring to provide PE redundancy)
- VRRP and VRRP-E
- Graceful restart for IP routing features

The node that is being upgraded goes through a hardware reset. This resets the packet processor, and traffic flowing through that specific node is disrupted.

How ISSU Works When Upgrading Stack Units

The checks and upgrade sequence for a typical 8-unit stack is shown in Figure 3. For a step-by-step procedure on performing an ISSU, refer to Upgrading a Stack with ISSU on page 54.

FIGURE 3 Stack Units to Be Upgraded



After you have downloaded release software, as described in Initial Steps on page 23 and Upgrade Process on page 35, you can check the sequence in which stack units will be upgraded using the **show issu sequence** command. The following example displays the ISSU upgrade sequence for the stack shown in Figure 3.

```
ICX7850-48F# show issu sequence
Stack units will be upgraded in the following order
ID      Type            Role
4       ICX7850-48F     standby
3       ICX7850-48F     member
2       ICX7850-48F     member
5       ICX7850-48F     member
6       ICX7850-48F     member
7       ICX7850-48F     member
8       ICX7850-48F     member
1       ICX7850-48F     active
```

All stack ISSU processes follow the same pattern. As reflected in the sample output, the stack in the example responds to the **show issu sequence** command in the following ways:

- Unit 4, the standby controller, is reloaded with the new image.
- Once the standby controller joins the stack, all member units from the standby controller to the active controller units (3 and 2) reload the new image.
- All members from the standby controller to the active controller in the other direction (units 5, 6, 7, and 8) reload the new image.

- Once all member units and the standby controller are reloaded with the new image, the active controller unit triggers a switchover, in which the old standby controller (unit 4) becomes the new active controller unit, and the old active controller (unit 1) becomes the new standby controller.
- The new active controller (unit 4) reloads the old active controller (unit 1) with the new image.
- Once the old active controller (unit 1) comes up as a member unit and rejoins the stack, standby controller election occurs, and the stack becomes fully functional with the upgraded image.

  NOTE
  If the stack unit configurations have priority settings, a final switchover is done to ensure that the unit with the highest priority becomes the active controller unit.

Pre-ISSU Compatibility Checks for a Traditional Stack

After ISSU is triggered, but before ISSU processing begins, a pre-ISSU compatibility check is executed.

The compatibility check determines whether the stack is ready for an upgrade. A successful compatibility check for a stack displays the passing results, as shown in the following table.

TABLE 13 Pre-ISSU Checks for a Traditional Stack

Check	Passing Result
Stacking Topology is Ring	Yes
Standby Present	Yes
Standby ready for upgrade	Yes
Flash use in progress	No
Stack interactive-setup in progress	No
Stack ZTP is configured	No
ISSU in progress or aborted	No
Election pending	No
Election in progress	No
Reload pending	No
CPU utilization high	No
All units in ready state	Yes
Primary Image is upgrade compatible	Yes
Secondary Image is upgrade compatible	Yes
Startup config and running config Same	Yes
Boot option present in running config	No
User in Config mode	No
POE-Firmware Download is in Progress	No
System ready for issu	If this flag is present, you can proceed with ISSU. Otherwise, check the conditions flagged by three asterisks (***) and make prescribed corrections to the device before performing an ISSU.

Upgrading a Stack with ISSU

The following examples for copying images represent typical use. Other options, such as manifest-based image copy, can also be used. Refer to Initial Steps on page 23 and Upgrade Process on page 35 for more information before performing the upgrade.

Complete the following steps to upgrade a stack using ISSU.

NOTE
By default, switches are booted from the primary partition.

1. Copy the images.
   a) Back up the running image to the secondary partition.

```
device# copy flash flash secondary
```

   b) Copy the new image from its server location to the primary partition.

```
device# copy tftp flash 10.10.10.10 SWR08090aufi.bin primary
```

   The IP address in the example is for the TFTP server. The address can be an IPv4 or IPv6 address. The .bin file is the name of the image file.
2. Check the sequence of the upgrade.

```
device# show issu sequence
Stack units will be upgraded in the following order
ID Type         Role
1 ICX7850-48F   standby
3 ICX7850-48F   member
4 ICX7850-48F   active
```

   The example shows the sequence for a three-unit stack.

3. Initiate the upgrade.

   Use the **issu primary** command, preferably with an error recovery option, if you downloaded the image to the primary partition of the flash.

   Or use the **issu secondary** command, preferably with an error recovery option, if you downloaded the image to the secondary partition.

   NOTE
   RUCKUS recommends using an error recovery option when upgrading.

   NOTE
   The issu command option **on-error reload-primary** shown in the following example specifies an automatic reload from the primary partition if there is an upgrade error. You can also specify the option **on-error reload-secondary** to reload from the secondary partition to bring the stack back up with the original image.

- Initiating the upgrade with error recovery.

```
device# issu primary on-error reload-primary
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
Proceed with upgrade? (enter 'y' or 'n'):
```

- Initiating the upgrade without error recovery (not recommended)

```
device# issu secondary
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
Proceed with upgrade? (enter 'y' or 'n'):
```

If an error occurs when the upgrade was initiated without error recovery, the error condition is marked by three asterisks.

```
device# issu primary
Stacking Topology is Ring               Yes
Standby Present                         No   ***
Standby ready for upgrade               No   ***
```

```
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System not ready for issu. Check error condition highlighted by "***" and rectify.
ISSU not in progress
```

4. Enter **y** when prompted to start the upgrade, or **n** to stop the process.

5. Wait for the upgrade to complete, and check the status. (You may check the status at any time.)

   The following **show issu status** command output indicates the successful completion of an ISSU upgrade.

```
device# show issu status
Last upgrade time 00:02:19.367 GMT+00 Tue Mar 20 2019
The older image before-ISSU SPR08090.bin
Stacking Topology is Ring               Yes
Standby Present                         Yes
Standby ready for upgrade               Yes
Flash use in progress                   No
Stack interactive-setup in progress     No
Stack ZTP is configured                 No
ISSU in progress or aborted             No
Election pending                        No
Election in progress                    No
Reload pending                          No
CPU utilization high                    No
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System ready for issu
ISSU not in progress
```

   The following example shows a status display for an upgrade that is in progress.

```
device# show issu status
ISSU Status: In Progress
Upgrade State: UNIT JOIN
Upgrade Option: issu primary
ID   Type          Role      State
1    ICX7850-48F   member    UPGRADING
3    ICX7850-48F   member    UPGRADE PENDING
4    ICX7850-48F   active    UPGRADE PENDING
```

   If the upgrade has not been initiated, the **show issu status** command displays information about whether the system is ready for the upgrade.

   The following example shows a status display for an aborted upgrade.

```
device# show issu status
ISSU Status: Aborted
Upgrade State: UPGRADE ABORT
Upgrade Option: issu primary
Reason for Abort: UNABLE TO UPGRADE
ID   Type          Role      State
1    ICX7850-48F   member    UPGRADE ABORT
3    ICX7850-48F   standby   UPGRADE PENDING
4    ICX7850-48F   active    UPGRADE PENDING
```

   The following example shows an unsuccessful ISSU that was aborted due to a hot swap error.

```
device# show issu status
 Abort info before recovery upgrade:
         Reason for abort                HOTSWAP ERROR
         Hotswap error with Unit 1
 Topology is Ring                        Yes
 Standby Present                         Yes
 Standby ready for upgrade               Yes
 Flash use in progress                   No
 Stack interactive-setup in progress     No
 ISSU in progress or aborted             No
 Election pending                        No
 Election in progress                    No
 Reload pending                          No
 CPU utilization high                    No
```

```
All units in ready state                Yes
Primary Image is upgrade compatible     Yes
Secondary Image is upgrade compatible   Yes
Startup config and Running Config Same  Yes
Boot option present in running config   No
User in Config mode                     No
POE-Firmware Download is in Progress    No
System ready for issu
ISSU not in progress
```

If the upgrade is aborted manually or if ISSU detects an abort condition (when the **issu** command is used without the **on-error** option), the stack is left as it is, and a manual recovery is required.

Summary ISSU Command Sequence for Upgrading a Stack

```
device# copy flash flash secondary
device# copy tftp flash 10.10.10.10 SWR0809a0ufi.bin primary
device# show issu sequence
device# issu primary on-error reload-primary
device# show issu status
```

ISSU Errors

There are several sources of errors that may be encountered during an ISSU, and there are two means of error recovery.

TABLE 14 Common Errors During ISSU

Error	Description
Hot-swap timeout	Unit hot-swap does not complete within the expected time.
Version synchronization timeout	Version information synchronization does not complete within the expected time.
Standby assignment timeout	After upgrading the current standby unit, the standby assignment does not occur within the expected time.
Standby assignment error	After upgrading the current standby unit, the expected unit was not elected as the new standby unit.
Image/boot source mismatch	After a unit upgrade, the image version and boot source did not match the expected version or boot source.
Unit fails to rejoin	The unit fails to rejoin the stack within the specified time after an upgrade.
Unit delete	The unit is detached from the stack while the ISSU is in progress.
Ping fail	A unit fails to respond to keepalive messages.

TABLE 15 Crash and Manual Abort Errors

Error Message	Description
Unit crash	If the **issu primary** command **on-error** option is specified, the unit that crashes is reloaded from the partition specified in the command. The active controller detects this condition as a unit delete and reloads all the existing stack members from the partition specified in the **issu primary** command **on-error** option.

TABLE 15 Crash and Manual Abort Errors (continued)

Error Message	Description
Active reload/crash	If the active controller reloads unexpectedly, or crashes while the ISSU is in progress, the stack units detect the loss of the active controller and abort the ISSU. If the **issu primary** command **on-error** option is specified, all units that were part of the stack at the time of the active controller crash are reloaded from the partition specified in the command. Any units that were being upgraded at the time of the active controller failover reload from the target partition given in the **issu primary** command. Once all units have booted and an active controller has been elected, if some units have a running image different from the active controller image, an image auto-copy is executed, and units are reloaded to ensure they are all running the same image.
Manual abort	If ISSU is aborted through the **issu abort** command, ISSU is stopped, and the stack is left in the current state for manual recovery. This behavior occurs whether ISSU is started with or without the **issu primary** command **on-error** option.

Error Recovery

There are two means for error recovery, one manual and one automatic:

- When ISSU is started with the **issu primary** or **issu secondary** command, the following results apply:
  - If an error occurs, the upgrade is aborted, and the stack is left for manual recovery. In this condition, it is likely that the running images on the stack units are different. After abort, image auto-copy is not executed.
  - Units continue with their current running image until the system is reloaded. As a result, a reload of the entire stack is required to bring it back to a functional state.
  - To ensure system stability, the stack is left in the aborted state. You must reload the system manually. If any of the stack units are reloaded individually, they cannot move to the Ready state. To execute a manual recovery, refer to Manual Error Recovery on page 60.
- The following points apply when ISSU is started with an **issu primary** or an **issu secondary** command that includes an **on-error reload primary** or an **on-error reload-secondary** option:
  - If an error occurs, the upgrade is aborted.
  - All the units in the stack are automatically reloaded to the partition specified by the **issu primary** command **on-error** option.
  - After the system reload, any units that were unreachable at the time of the ISSU abort may have an image that is different from the other units. When these units rejoin the stack, an image auto-copy is executed for any units with a mismatched image, and they are reloaded after the auto image copy completes.

Manual Error Recovery

If an error is detected during the upgrade, ISSU is aborted. In this case, the recommended procedure is to reload the stack to the old or new image from the primary or secondary partition, and then use the **boot system flash** command to reload the stack.

Complete the following steps to manually recover from an ISSU error.

1. Reload to the primary partition.

```
device# boot system flash primary
```

2. Reload to the secondary partition.

```
device# boot system flash secondary
```

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com